OWASP amass KULLANIM KILAVUZU

Yazar: Özgür Koca, ozgurkoca.com, Haziran 2022

OWASP Amass, açık kaynak bilgi toplama ve aktif keşif teknikleri kullanarak saldırı hedeflerinin ağ haritalamasını ve harici varlık keşfini gerçekleştirir. Aracın alt alan adlarını bulmak için kullandığı tekniklere buradan bakabilirsiniz. Bir OWASP projesi olan Amass, açık kaynak istihbaratı (OSINT) alanında kullanılan önemli blueteam araçlarından birisidir. Go dilinde yazılmış olan aracın temel odağı alan adı (domain name) istihbaratı ve keşfi yapmaktır.

OWASP Amass aracı, veri kaynaklarını kazıyarak, özyinelemeli kaba kuvvet uygulayarak, web arşivlerini tarayarak, adlara izin vererek/değiştirerek ve ters DNS taraması yaparak alt alan adlarını elde eder. Ek olarak, Amass, ilişkili ağ bloklarını ve ASN'leri keşfetmek için çözümleme sırasında elde edilen IP adreslerini kullanır. Tüm bilgiler daha sonra hedef ağların haritalarını oluşturmak için kullanılır. Amass'in kullandığı araştırma ve keşif teknikleri şunlardır:

- **Değişiklik/Permutasyon**: Bulunan alt alan adlarında ilkel değişiklikler (dev1 <-> dev2). musteri1.domain.com gibi bir alt alan gördüğünde musteri2.domain.com gibi sırasal alt alanları da tarar.
- **Bulanık etiket/string arama**: Ekleme çıkarma (dev <-> dav). dev.domain.com gibi bir alt alan gördüğünde basit harf değişiklikeri ile olası alt domainleri bulmayı dener.
- **Özeyineli kaba kuvvet**: API'ler ve WEB arşivlerini araştırma. wayback.com ve archiveit.com gibi arşivlerden alt domain araştırması yapar. Keşif yaptığı veri kaynakları aşağıda yer alıyor. Bunlardan bazıları API key'e ihtiyaç duyan limitli servislerdir.
- **Aktif teknikler**: HTTP TLS/SSL sertifikalarını indirme. Common Name kısmında altalan adı bilgileri yer alır.
- **Zones**: Zone transferlerini izleme ve zone walking (NSEC kayıtları).
- **Public kaynaklar**: Web arşivleri, pastebin, version control ve sosyal medya web siteleri.
- **Certificate Transparancey (CT) logs'ları**: CT sertifikanın güvenli ya da zararlı olup olmadığını doğrulamak ve sertifikaları takip etmek için kullanılan bir framework'tür. Domain için tanımlanmış sertifikaları kullanarak keşif yapmaya çalışır.
- **HTTP CSP (Content Security Policy) başlıkları**: Poliçelere alt alanlar (sub domains) da dahil edildiğinde CSS saldırılarından korunmak için burada beyaz listeye alınırlar. Bu beyaz listelerde amass için bir veri kaynağı oluşturur.

Amass'ın araştırma ve keşif yaparken kullandığı veri kaynakları aşağıda yer alıyor. amass'ın halihazırdaki veri kaynaklarını ve kullanılabilirlik durumlarını görmek için aşağıdaki komutu çalıştırabilirsiniz.

```
amass enum -list
```

Amass 50 civarında veri kaynağını kullanabilir, bunlardan bazıları ücretsiz, bazıları deneme kullanımına sahip bazıları da oldukça pahalı servislerdir. En başarılı veri kaynaklarını takip etmek için komutlarınıza -src parametresini ekleyebilirsiniz. Böylece hangi kaynağın ne sıklıkla sonuç döndürdüğünü takip edebilirsiniz.

TEKNIK	VERI KAYNAĞI
API'LER	360PassiveDNS, Ahrefs, AnubisDB, BinaryEdge, BufferOver, BuiltWith, C99, Chaos, CIRCL, Cloudflare, DNSDB, DNSRepo, Detectify, FOFA, FullHunt, GitHub, GitLab, Greynoise, HackerTarget, Hunter, IntelX, LeakIX, Maltiverse, Mnemonic, N45HT, PassiveTotal, PentestTools, Quake, Shodan, SonarSearch, Spamhaus, Spyse, Sublist3rAPI, ThreatBook, ThreatCrowd, ThreatMiner, Twitter, URLScan, VirusTotal, ZETAlytics, ZoomEye
SERTIFIKALAR	Active pulls (optional), Censys, CertSpotter, Crtsh, Digitorus, FacebookCT, GoogleCT
DNS	Brute forcing, Reverse DNS sweeping, NSEC zone walking, Zone transfers, FQDN alterations/permutations, FQDN Similarity-based Guessing
YÖNLENDIRME	ARIN, BGPTools, BGPView, IPdata, IPinfo, NetworksDB, RADb, Robtex, ShadowServer, TeamCymru
SCRAPING	AbuseIPDB, Ask, Baidu, Bing, DNSDumpster, DuckDuckGo, Gists, HackerOne, HyperStat, IPv4Info, PKey, RapidDNS, Riddler, Searchcode, Searx, SiteDossier, Yahoo
WEB ARŞIVLERI	AlienVault, AskDNS, DNSlytics, ONYPHE, SecurityTrails, SpyOnWeb, Umbrella, WhoisXMLAPI
WHOIS KAYITLARI	AlienVault, AskDNS, DNSlytics, ONYPHE, SecurityTrails, SpyOnWeb, Umbrella, WhoisXMLAPI

Amass oldukça kapsamlı ve gelişmiş bir araçtır. Araç kendi içinde intel, enum, viz, track ve db olmak üzere 5 alt komutu barındırır. **intel** komutu hedef üzerinde keşif yapar. Hedef için başlangıç noktası belirlemek için faydalıdır. **enum** olası saldırı noktalarını belirlemek için hedefin haritasını çıkartır. **viz** elde edilen sonuçları görselleştirerek daha iyi bir analiz yapılmasına yardımcı olur. **track** hedef üzerinde zamanla oluşan değişiklikleri takip etmek ve karşılaştırmak için kullanılır. amass tüm istihbarat ve tarama sonuçlarını kendi veritabanına kaydeder. **db** alt komutu ise bu veritabanına erişmek ve sorgulama yapmak için kullanılır. amass'in tüm komut ve seçeneklerine ulaşmak için döküman sayfasına bakabilirsiniz. Bu başlıkta sadece temel kullanımlarını örneklendireceğim.

Amass Alt Komutları

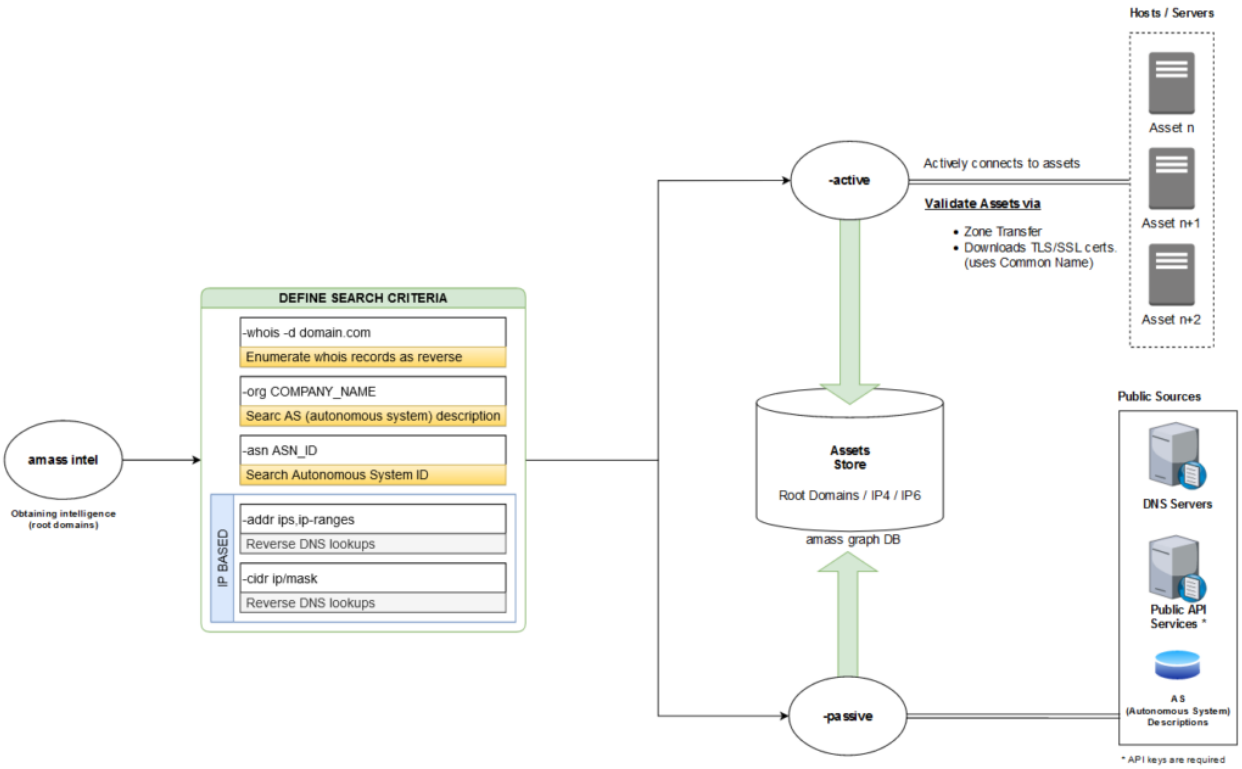
- **amass intel**: Kök alan adlarını (alt domain'ler değil), ASN'leri keşfeder, reverse WHOIS & DNS sorguları yapar. Hedef organizasyonun araştırılması için açık kaynak istihbaratı yapar.
- **amass enum**: Altalanları keşfetme, hızlı mod (passive), normal mod, DNS resolution/validation tekniklerini kullanarak İnternet'e açık sistemlerin DNS kayıtlarını çıkartır ve haritalamasını yapar.
- **amass viz**: Görsel grafikler oluşturur, görsel inceleme için iyidir. Maltego'yu destekler. Yapılan keşif ve araştırmaların görsel bir diyagramını oluşturur.
- **amass track**: Taramalar arasında tarihsel karşılaştırma yapmayı, yeni veya güncellenmiş varlıkları görmeyi sağlar.
- **amass db**: Amass yaptığı tüm aktif ve pasif keşifleri kendi veritabanında saklar. Bu kayıtlara daha sonradan erişmek için db komutu kullanılır.

intel komutu

Amass intel alt komutu/modülü, kuruluş hakkında açık kaynak istihbaratı toplamaya yardımcı olabilir ve kuruluşla ilişkili daha fazla kök etki alanı (domain name) adı bulmanıza olanak tanır. Bu alt komutun mevcut seçeneklerini görmek için, onu terminale yazmanız yeterlidir:

```
$ amass intel
[...]
Usage: amass intel [options] [-whois -d DOMAIN] [-addr ADDR -asn ASN -cidr CIDR]
  -active
        Attempt certificate name grabs
  -addr value
        IPs and ranges (192.168.1.1-254) separated by commas
  -asn value
        ASNs separated by commas (can be used multiple times)
  -cidr value
        CIDRs separated by commas (can be used multiple times)
  -org string
        Search string provided against AS description information
  -whois
        All provided domains are run through reverse whois
[...]
```

Bu noktada, Amass'ın bir başka büyük avantajının, tüm alt komutların argüman tutarlılığını korumaya çalışması olduğunu belirtmekte fayda var. İlerleyen paragraflarda alt komutların parametreleri yer alıyor, çoğunun ortak kullanıldığını görebilirsiniz. Aşağıdaki şema amass intel'in çalışma mantığını temel olarak göstermektedir.



Bu alt komut, Amass'ın yapılandırma dosyasında açıkça devre dışı bırakılmadığı sürece, kuruluşa ait istihbarat ve üst etki alanlarını elde etmek için varsayılan olarak WHOIS ve IPv4Info gibi bir dizi bilgi toplama tekniği ve veri kaynağı kullanacaktır. GitHub deposunda örnek bir Amass yapılandırma dosyası mevcuttur.

```
$ amass intel -whois -d owasp.org
appseceu.com
owasp.com
appsecasiapac.com
appsecnorthamerica.com
appsecus.com
[...]
owasp.org
appsecapac.com
appsecla.org
[...]
```

Veri kaynaklarına manuel olarak göz atarak da yukarıdaki sonuçların bazılarını onaylayabilirsiniz. Aşağıdaki ekran görüntüsünde, "OWASP Foundation" için ters Whois araması yaptık ve ViewDNS'e (aynı zamanda Amass'ın veri kaynaklarının bir parçasıdır) benzer alan adları sorduk:

https://viewdns.info/reversewhois/?q=owasp%20foundation

```
Reverse Whois results for OWASP Foundation
==============

There are 15 domains that matched this search query.
These are listed below:
```

Domain Name	Creation Date	Registrar
appseccali.org	2013-07-16	GODADDY.COM, LLC
appseccalifornia.org	2013-07-16	GODADDY.COM, LLC
appsecil.com	2017-09-01	GODADDY.COM, LLC
appsecil.info	2017-09-01	GODADDY.COM, LLC
appsecil.org	2017-09-01	GODADDY.COM, LLC
appsecli.info	2017-09-01	GODADDY.COM, LLC
appsecli.org	2017-09-01	GODADDY.COM, LLC

Amass intel ile arama yaparken, her zaman daha fazla yapılandırma seçeneğiyle çalıştırabilirsiniz, örneğin --active argümanı ile zone transferi dener ve bilgileri çıkarmak için SSL/TLS sertifikalarını almak üzereilgili sunucuya bağlanmasını sağlayabilirsiniz. Yalnız bunu yapmadan önce hedefe karşı aktif aramalar yapma yetkiniz olduğundan emin olun.

Bu noktada, bazı konfigürasyon bayraklarının diğerleriyle birlikte çalışmayacağını ve bu durumda Amass'ın onları görmezden geleceğini belirtmekte fayda var.

Amass'ın bulguları her zaman doğru olmayabilir, bunun çeşitli nedenleri vardır, örneğin Amass tarafından kullanılan veri kaynakları tutarlı veya güncel olmayabilir. Amass, DNS sorgularını kullanarak bilgileri daha fazla doğrulamaya çalışır. Amass iyi bir iş çıkarsa da, kullanıcılar hedefle ilgili görünmeyen sonuçlar üzerinde yine de daha fazla doğrulama kontrolü yapmalıdır. Bu, aşağıdakiler gibi çeşitli yöntemler kullanılarak gerçekleştirilebilir:

- Etki alanlarını çözümlemek için yardımcı programları kullanın (ör. dig, nslookup).
- Kurumsal ayrıntıları doğrulamak için WHOIS aramaları yapın.
- Arama motorlarında ana etki alanları gibi arama bulgularını kullanın.

```
amass intel -org TURKIYE
```

Turkiye kelimesi ile alakalı ASN ID'leri getirir. Bu tarz string araştırmaları çoğu zaman yeterince sonuç döndürmeyebilir. Araştırmanın aktif yöntemler de kullanılarak gerçekleştirilmesini istiyorsanız -active anahtarını da ekleyebilirsiniz. Yukarıdaki komut ASN açıklamalarında Turkiye kelimesini arayacak ve ilişkili ASN'leri getirecektir.

Org anahtarı verilen ifade ile ilişkili ASN ID (Autonomous system/Özerk Sistem)'lerini araştırır. -org parametresi ile belirtilen string, AS kayıtları içinde aranır ve ASN ID'si bulunur. ASN ID, İnternet Atanmış Numaralar Kurumu (IANA) tarafından atanan özerk sistem numarasıdır, dünya çapında benzersiz bir 16 haneli kimlik numarası ile gösterilir. Bir AS (Özerk Sistem) tek bir yönlendirme politikasına sahip (rfc1930) geniş bir ağ veya ağ grubunu ifade eder. ASN ID'de bunları tanımlar. Örneğin TTNET'e ait ağın ASN numarası 9121, CloudFlare'in 13335, ULAKNET'in 8517 ve Amazon'un 16509'dur. Ağlar arasında yönlendirme yapılması gerektiğinde, büyük yönlendiriciler (router) bu ASN numaralarından faydalanır.

Şimdi de bulduğumuz bir ASN içindeki alan adlarını bulmaya çalışalım. Aşağıdaki komutu inceleyin.

```
amass intel -active -src -ip -asn 8517 -p 80,443
```

ASN numarası 8517 olan otonom ağda (ULAKNET) yer alan domainlerin, 80 ve 443 portlarına aktif teknikleri (-active) kullanarak bir keşif yapacaktır. Aktif keşif için TLS/SSL sertifikalarını kullanacaktır. amass belirtilen ASN'ye ait tüm IP adreslerine bağlanacak SSL sertifikasını çekecek ve SSL sertifikasının ilişkili olduğu domain'i listeleyecektir. Ayrıca bulduğu domain'lerin kaynaklarını (-src) ve ip (-ip) adreslerini de görüntüleyecektir.

```
amass intel -active -ip -src -cidr 193.140.28.0/24 -p 80,443
```

-cidr parametresi ile bir ip aralığı bildirilmiştir. 24 sayısı ağ maskesini ifade eder ve 255.255.255.0'a karşılık gelir. amass 193.140.28.1 ile 193.140.28.254 arasındaki ip adresleri için farklı kaynaklarda araştırma ve keşif yaparak, bu IP'lere yönlendirilmiş alan adlarını tespit edecek ve listeleyecektir. Ayrıca aktif keşif 80 ve 443 portları için TLS/SSL sertifikaları kullanılarak yapılacaktır. Herbir IP adresine bağlanıp SSL sertifikalarını çekecek ve sertifikada geçen alan adlarını listeleyecektir.

```
amass intel -active -ip -src -cidr 74.6.0.6/16 -addr 74.6.231.20-21 -p 80,8080
```

Aktif teknikler kullanılarak 74.6.0.6/16 ağındaki bilgisayarları tarayacak. Bulunan domainlerin ip adresini ve kaynağını listeleyecektir. 74.6.231.20-21 aralığındaki bilgisayarlara ters DNS sorgusu gerçekleştirecek.

```
amass intel -whois -d yahoo.com
```

Verilen domain (-d)'in veya domain listesinin (-df) WHOIS kayıtlarını tersine araştırarak alan adlarını bulmaya çalışır. Bu örnekte amass, yahoo.com'un WHOIS kayıtlarına erişir ve bu WHOIS kayıtları ile aynı olabilecek diğer kuruluşların kök domain'lerini bulmaya çalışır. Bir organizasyona/şirkete ait diğer domain'leri bulmak için kullanışlıdır lakin WHOIS kayıtları herzaman doğru bilgiler içermeyebilir veya gizli tutulmuş olabilir.

```
amass intel -asn 8517 -whois -d omu.edu.tr
```

Bu komut ASN ID'si 8517 olan ULAKNET otonom ağında, WHOIS kayıtları aynı olan diğer domainleri arar.

Aşağıda intel komutunun seçenekleri ve kullanım alanlarını gösteren bir tablo yer alıyor.

SEÇENEK	AÇIKLAMA	ÖRNEK
-ACTIVE	Aktif yöntemleri kullanır. Zone transferi dener, SSL/TLS sertifikalarını almak için hedef sunucuya bağlanır.	amass intel -active -addr 192.168.2.1-64 -p 80,443,8080
-ADDR	IP aralıkları belirtir. Aralıklar virgülle ayrılır.	192.168.2.1-64,192.168.3.10-254
-ASN	ASN ID bildirir. ASN ID, IANNA tarafından büyük bilgisayar ağlarına atanan benzersiz bir numaradır.	amass intel -asn 13374,14618
-CIDR	Bir ağ tanımlar. Taksim işaretinden sonraki sayı ağ maskesini tanımlar.	amass intel -cidr 104.154.0.0/15
-CONFIG	Tarama yapılandırma dosyasının konumunu belirtir.	amass intel -config config.ini
-D	Virgül ile ayrılmış alan adları.	amass intel -whois -d example.com
-DF	Kök alan adlarını bir dosyadan besler.	amass intel -whois -df domains.txt
-DIR	Tarama sonularının saklanacağı veritabanını içeren dizinin yolunu belirtir.	amass intel -dir PATH -cidr 104.154.0.0/15
-EF	Araştırma yapılırken kullanılmayacak veri kaynaklarının bir listesinin yer aldığı dosyanın yolu.	amass intel -whois -ef exclude.txt -d example.com
-EXLUDE	Taramada kullanılmayacak veri kaynaklarının listesi. Virgülle ayrılarak belirtilir.	amass intel -whois -exclude crtsh -d example.com
-IF	Taramada kullanılacak veri kaynaklarının bir listesinin yer aldığı dosyanın yolu.	amass intel -whois -if include.txt -d example.com
-INCLUDE	Taramada kullanılacak veri kaynaklarının listesi. Virgülle ayrılarak yazılır.	amass intel -whois -include crtsh -d example.com
-IP	Keşfedilen alan adlarının IP adreslerini de gösterir.	amass intel -ip -whois -d example.com
-IPV4	Keşfedilen alan adlarının IPv4 adreslerini de gösterir.	amass intel -ipv4 -whois -d example.com
-IPV6	Keşfedilen alan adlarının IPv6 adreslerini de gösterir.	amass intel -ipv6 -whois -d example.com
-LIST	Keşifte kullanılacak veri kaynaklarını listeler.	amass intel -list
-LOG	Hataların kaydedileceği günlük dosyasının yolunu bildirir.	amass intel -log amass.log -whois -d example.com
-MAX-DNS-QUERIES	En fazla eşzamanlı DNS sorgusu sayısı.	amass intel -max-dns-queries 200 -whois -d example.com
-O	Çıktının kaydedileceği dosyanın yolu.	amass intel -o out.txt -whois -d example.com
-ORG	AS açıklamasında araştırılacak string ifade.	amass intel -org Facebook
-P	Virgülle ayrılmış port numaraları.	amass intel -cidr 104.154.0.0/15 -p 443,8080
-R	Keşif sırasında kullanılacak DNS sunucuları bildirir.	amass intel -r 8.8.8.8,1.1.1.1 -whois -d example.com

-RF	Keşif sırasında kullanılacak DNS sunucuların listesinin yer aldığı dosyanın yolunu bildirir.	amass intel -rf data/resolvers.txt -whois -d example.com
-SRC	Keşfedilen alanların hangi kaynaktan temin edildiğini gösterir.	amass intel -src -whois -d example.com
-TIMEOUT	Keşif sırasında dikkate alınacak zaman aşımı süresi.	amass intel -timeout 30 -d example.com
-WHOIS	WHOIS bilgileri benzer diğer alan adlarını araştırır.	amass intel -whois -d example.com

amass enum komutu

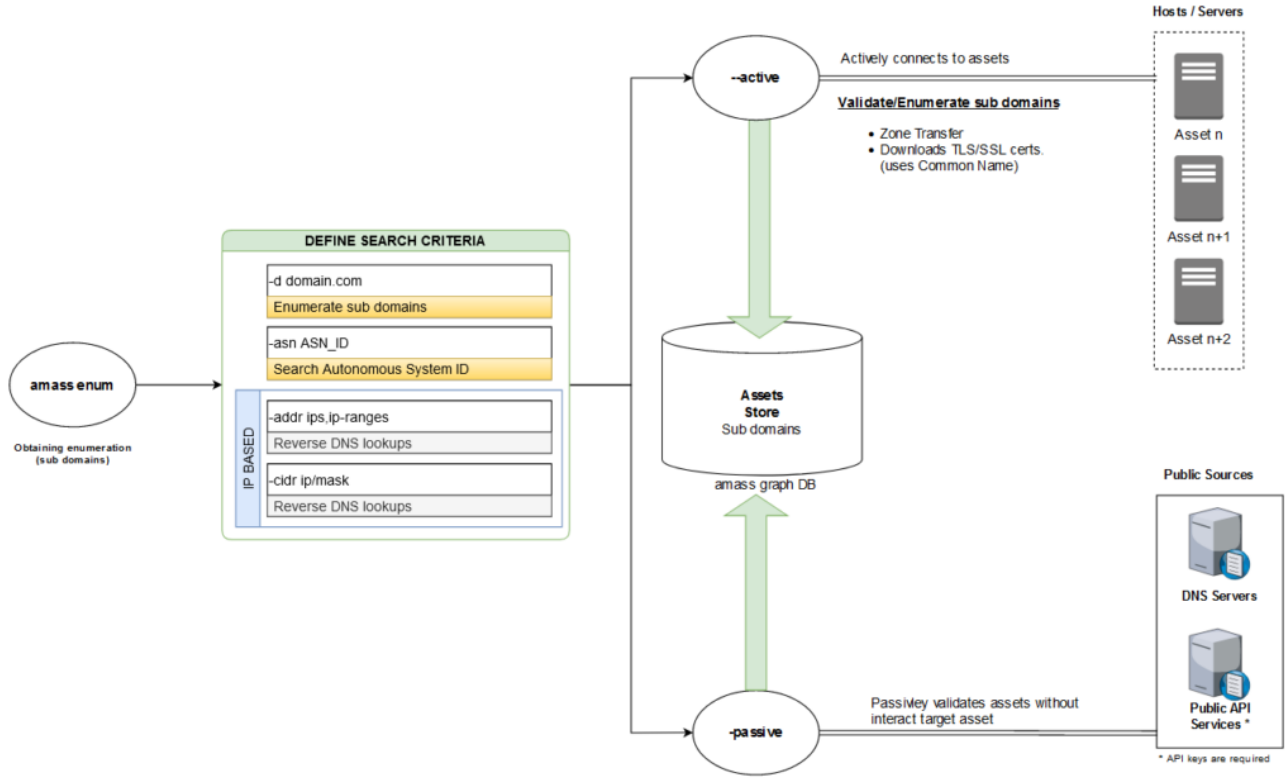
Amass enum, pasif veya aktif bir modda çalıştırılabilir. Pasif mod çok daha hızlıdır, ancak Amass, alt alanları çözümleyerek DNS bilgilerini doğrulamayacaktır. "-passive" bayrağını kullanarak pasif olarak çalıştırabilirsiniz ve DNS çözümlemesi ve doğrulaması gibi birçok tekniği veya yapılandırmayı etkinleştiremezsiniz. Bazen aktif mod yerine pasif modu seçmek gerekebilir, örneğin:

- Değişiklikler için hedef kapsamını sürekli olarak izlemeniz gerektiğinden veya bir kimlik avı etkileşimi üzerinde çalıştığınız ve alt etki alanları aradığınız için kullanılmış ve gelecekte yeniden kullanılabilecek tüm olası alt etki alanlarını bilmeniz gerekir.
- DNS bilgilerini daha sonraki bir aşamada doğrulamak ve hızlı bir şekilde biriktirme sonuçlarına ihtiyaç duyabilirsiniz.
- Bir güvenlik angajmanının kısıtlamaları veya gereksinimleri nedeniyle, yalnızca pasif bilgi toplama gerçekleştirmeniz gerekebilir.

Bu alt komutun mevcut seçeneklerini görmek için, onu terminale yazmanız yeterlidir:

```
Usage: amass enum [options] -d DOMAIN

  -active
        Attempt zone transfers and certificate name grabs
  -addr value
        IPs and ranges (192.168.1.1-254) separated by commas
  -d value
        Domain names separated by commas (can be used multiple times)
  -cidr value
        CIDRs separated by commas (can be used multiple times)
  -asn value
        ASNs separated by commas (can be used multiple times)
```



Aşağıdaki örnekte, Owasp.org'da pasif olarak alt alan adları arıyoruz ve Amass'tan her bir alt alan adını bulduğu veri kaynaklarını görüntülemesini istiyoruz:

```
$ amass enum -passive -d owasp.org -src
[...]
[ThreatCrowd]     update-wiki.owasp.org
[...]
BufferOver]      my.owasp.org
[Crtsh]           www.lists.owasp.org
[Crtsh]           www.ocms.owasp.org
[...]
Querying VirusTotal for owasp.org subdomains
Querying Yahoo for owasp.org subdomains
[...]
```

Bu alt komut, araştırma yapılırken DNS keşfi ve ağ haritalama gerçekleştirecektir. Bu noktada, Amass intel komutunun bir kuruluşun sahip olduğu IP aralıklarını, ASN'leri ve ana etki alanlarını toplamaya yardımcı olmasına rağmen, Amass enum'un tüm alt etki alanlarını tanımlayacağını belirtmekte fayda var.

Amass'ı aktif konfigürasyon modunda kullanmak, tüm DNS keşif tekniklerini etkinleştirebildiğiniz için daha doğru sonuçlara sahip olacağınız ve daha fazla varlığın keşfedilebileceği anlamına gelir. "Etkin yapılandırma modu" ile, SSL/TLS hizmetlerinin zone transfer ve bağlantı noktası (port) taramalarını yaparak sertifika alanlarından alt domainleri araştıracaktır (örn.: Common Name).

Aşağıdaki komut (ayrıntılı bir açıklaması aşağıdadır), "-active" bayrağının etkinleştirilmesiyle birlikte birden çok yolla (kelime listesi, maskeler, vb.) alt etki alanı kaba zorlaması

gerçekleştirdiğinden genel olarak etkin olarak kabul edilebilir. Tüm bulgular, varsayılan veya belirtilen çözümleyiciler kullanılarak Amass tarafından doğrulanacaktır:

Aşağıda bulunan tüm ayarlar bu alt komutla ilgilidir. Yapılandırma için aşağıdaki bayraklar kullanılabilir:

Seçenek	***Açıklama***	***Örnek***
-active	Aktif yöntemleri kullanır. Zone transferi dener, SSL/TLS sertifikalarını almak için hedef sunucuya bağlanır.	amass enum -active -d example.com -p 80,443,8080
-aw	Alt domain alternatifleri üretmek için alternatif kelime dosyasının yolunu bildirir.	amass enum -aw PATH -d example.com
-bl	Keşfi yapılmayacak altalanların kara listesini bildirir.	amass enum -bl blah.example.com -d example.com
-blf	Kara listedeki alt alanların listesinin bulunduğu dosyanın patikasını belirtir.	amass enum -blf data/blacklist.txt -d example.com
-brute	Alt alan keşfinde kaba kuvvet kullanır.	amass enum -brute -d example.com
-config	INI yapılandırma dosyasının yolunu belirtir.	amass enum -config config.ini
-d	Virgül ile ayrılmış alan adları.	amass enum -d example.com
-df	Kök alan adlarını bir dosyadan besler.	amass enum -df domains.txt
-dir	Tarama sonularının saklanacağı veritabanını içeren dizinin yolunu belirtir.	amass enum -dir PATH -d example.com
-ef	Araştırma yapılırken kullanılmayacak veri kaynaklarının bir listesinin yer aldığı dosyanın yolu.	amass enum -ef exclude.txt -d example.com
-exclude	Taramada kullanılmayacak veri kaynaklarının listesi. Virgülle ayrılarak belirtilir.	amass enum -ef exclude.txt -d example.com
-if	Taramada kullanılacak veri kaynaklarının bir listesinin yer aldığı dosyanın yolu.	amass enum -ef exclude.txt -d example.com
-include	Taramada kullanılacak veri kaynaklarının listesi. Virgülle ayrılarak yazılır.	amass enum -include crtsh -d example.com
-ip	Keşfedilen alan adlarının IP adreslerini de gösterir.	amass enum -ip -d example.com
-ipv4	Keşfedilen alan adlarının IPv4 adreslerini de gösterir.	amass enum -ip -d example.com
-ipv6	Keşfedilen alan adlarının IPv6 adreslerini de gösterir.	amass enum -ip -d example.com
-json	JSON biçimli kaydedilecek çıktı dosyasının yolunu tanımlar.	amass enum -json out.json -d example.com
-list	Keşifte kullanılacak veri kaynaklarını listeler.	amass enum -list
-log	Hataların kaydedileceği günlük dosyasının yolunu bildirir.	amass enum -log amass.log -d example.com
-max-dns-queries	En fazla eşzamanlı DNS sorgusu sayısı.	amass enum -max-dns-queries 200 -d example.com

-dns-qps	Tüm alan adı çözümleyicilerinde (DNS sunucu) saniye başına maksimum DNS sorgusu sayısı.	amass enum -dns-qps 200 -d example.com
-rqps	Her güvenilmeyen çözümleyici için saniye başına maksimum DNS sorgusu sayısı.	amass enum -dns-qps 200 -d example.com
-trqps	Her güvenilir çözümleyici için saniyede maksimum DNS sorgusu sayısı	amass enum -trqps 20 -d example.com
-min-for-recursive	Özyinelemeli kaba zorlamadan önce görülen alt alan etiketleri (Varsayılan: 1)	amass enum -brute -min-for-recursive 3 -d example.com
-max-depth	Kaba zorlama için maksimum alt alan etiketi sayısı	amass enum -brute -max-depth 3 -d example.com
-nf	Halihazırda bilinen alt alan adlarını sağlayan bir dosyanın yolu (diğer araçlardan/kaynaklardan)	amass enum -nf names.txt -d example.com
-noalts	Alternatif alt alan adı üretmeyi devre dışı bırakır.	amass enum -noalts -d example.com
-norecursive	Özyinelemeli kaba kuvveti devre dışı bırakır.	amass enum -brute -norecursive -d example.com
-o	Metin çıktı dosyasının yolunu belirtir.	amass enum -o out.txt -d example.com
-oA	Tüm çıktı dosyalarını adlandırmak için kullanılan yol öneki.	amass enum -oA amass_scan -d example.com
-passive	Tamamen pasif bir yürütme gerçekleştirir.	amass enum --passive -d example.com
-p	Virgülle ayrılmış port numaraları.	amass enum -d example.com -p 443,8080
-r	Keşif sırasında kullanılacak DNS sunucuları bildirir.	amass enum -d example.com -p 443,8080
-tr	Güvenilir DNS çözümleyicilerinin IP adresleri (birden çok kez kullanılabilir)	amass enum -tr 8.8.8.8,1.1.1.1 -d example.com
-rf	Keşif sırasında kullanılacak DNS sunucuların listesinin yer aldığı dosyanın yolunu bildirir.	amass enum -tr 8.8.8.8,1.1.1.1 -d example.com
-trf	Güvenilir DNS çözümleyicileri sağlayan bir dosyanın yolunu belirtir.	amass enum -trf data/trusted.txt -d example.com
-src	Keşfedilen alanların hangi kaynaktan temin edildiğini gösterir.	amass enum -src -d example.com
-timeout	Keşif sırasında dikkate alınacak zaman aşımı süresi.	amass enum -timeout 30 -d example.com
-w	Farklı bir wordlist dosyasının yolunu bildirir.	amass enum -brute -w wordlist.txt -d example.com

enum komutunun en yaygın kullanım şekli aşağıdaki gibidir. Bu komut verildikten sonra amass meb.gov.tr alan adına ait alt alan adlarını internetten araştırmaya başlar. Sorabildiği tüm veri kaynaklarına sorar ve bir yığın alt alan adı döndürür.

```
amass enum -d meb.gov.tr
amass enum -passive -d yahoo.com -config ./passive-config.ini
```

Bu taramada DNS çözümlemesi yapılmadan (-passive) bir tarama gerçekleştirilir. passive-config.ini dosyasında pasif bilgi edinme kaynaklarının listesi ve API anahtarlarının yer aldığı varsayılmıştır. -passive seçeneği -active'e göre daha hızlı fakat daha az sonuç döndürür.

-v parametresini kullanarak amass.log dosyasının detay seviyesini artırabilir, uygularken amass'ın özelliklerini daha iyi kavrayabilirsiniz. Düzgün çalışmayan veri kaynaklarını tespit etmeyi, IP adresinizi bloklayan servisleri ve düzgün çalışmayan DNS çözümleyicilerini görmenizi sağlar.

amass track komutu

Bir hedefin saldırı yüzeyini (attack surface) izlemek için aynı hedef(ler)e ait keşifler arasındaki farkları gösterir. Bu alt komut, yalnızca 'output_directory' ve yapılandırma dosyasında belirtilen uzak veritabanı ayarlarından yararlanır.

Bu alt komutun mevcut seçeneklerini görmek için, onu terminale yazmanız yeterlidir:

```
Usage: amass track [options] -d domain
 -d value
        Domain names separated by commas (can be used multiple times)
 -history
        Show the difference between all enumeration pairs
  -last int
        The number of recent enumerations to include in the tracking
```

Seçenek	***Açıklama***	***Örnek***
-config	INI yapılandırma dosyasının yolunu belirtir.	amass track -config config.ini
-d	Virgül ile ayrılmış alan adları.	amass track -d example.com
-df	Kök alan adlarını bir dosyadan besler.	amass track -df domains.txt
-dir	Tarama sonularının saklandığı veritabanını içeren dizinin yolunu belirtir.	amass track -df domains.txt
-history	Keşifler arasındaki farkları gösterir.	amass track -history
-last	İzlemeye dahil edilecek son keşiflerin sayısı.	amass track -last 2
-since	Belirtilen tarihten önceki tüm numaralandırmaları hariç tut (biçim: 01/02 15:04:05 2006 MST)	amass track -since TARIH

```
amass track -d yahoo.com -last 2
```

Yukarıdaki komut yahoo.com domain'inin son iki taramasını karşılaştırır.

amass viz komutu

Toplanan bilgileri kullanarak görsel ağ grafikleri oluşturur. Bu görselleştirme özellikle kapsamlı sonuçlar döndüren geniş taramalarda varlıklar arasındaki ilişkileri yorumlamak için faydalıdır. Bu alt komut, yapılandırma dosyasından yalnızca 'output_directory' ve uzak grafik veritabanı ayarlarından yararlanır.

Görselleştirme için oluşturulan dosyalar varsayılan olarak geçerli çalışma dizininde oluşturulur. DNS ve altyapı bulgularını ağ grafiği olarak çıktılamak için kullanılabilecek anahtarlar şunlardır:

Seçenek	***Açıklama***	***Örnek***
-config	INI yapılandırma dosyasının yolunu belirtir.	amass viz -config config.ini -d3
-d	Virgül ile ayrılmış alan adları.	amass viz -d3 -d example.com
-d3	D3.js v4 biçimli HTML simulasyon dosyası oluşturur.	amass viz -d3 -d example.com
-df	Kök alan adlarının yer aldığı dosyanın yolunu tanımlar.	amass viz -d3 -df domains.txt
-dir	Graph veritabanını içeren dizinin yolunu tanımlar.	amass viz -d3 -dir PATH -d example.com
-enum	Tarama sonuçları veritabanından indeks numarası ile bir keşif tanımlar.	amass viz -enum 1 -d3 -d example.com
-o	Çıktı dosyalarının kaydedileceği dizinin yolunu tanımlar.	amass viz -d3 -o OUTPATH -d example.com
-oA	Çıktı dosyaları için bir ön ek tanımlar.	amass viz -d3 -oA example -d example.com
-gexf	Graph Exchange XML Format (GEXF) biçimli çıktı verir.	amass viz -gexf -d example.com
-graphistry	Graphistry JSON biçimli çıktı verir.	amass viz -graphistry -d example.com
-maltego	Maltego Graph Table biçimli CSV dosyasını çıktı verir.	amass viz -maltego -d example.com

```
amass viz -d yahoo.com -d3 -o yahoo
```

Yukarıdaki komut yahoo.com alan adına ait tüm sonuçları HTML biçimli bir dosyada ilişkisel bir grafikle görüntüler. Grafik d3 javascript kütüphanesi kullanılarak oluşturulur. -o seçeneği ile çıktının yahoo dizinine kaydedilmesi sağlanmıştır. vizz komutu Maltego, XML ve JSON biçimlerinde de çıktı verebilir.

amass db komutu

Yapılan her tarama için keşif verilerini görüntülemenizi sağlayan bir komuttur. Veritabanının görüntülenmesini ve işlenmesini gerçekleştirir. Bu alt komut, yapılandırma dosyasından yalnızca 'output_directory' ve uzak veritabanı ayarlarından yararlanır. Veri tabanındaki keşift bulgularıyla etkileşim için kullanım seçenkleri şunlardır:

SEÇENEK	**AÇIKLAMA**	**ÖRNEK**
-CONFIG	INI yapılandırma dosyasının yolunu belirtir.	amass db -config config.ini
-D	Virgül ile ayrılmış alan adları.	amass db -d example.com
-DF	Kök alan adlarını bir dosyadan besler.	amass db -df domains.txt
-DIR	Tarama sonuçlarını içeren veritabanı dizininin yolunu belirtir.	amass db -dir PATH
-ENUM	Listeden bir dizin sıra numarası aracılığıyla keşif bilgisi getirir.	amass db -enum 1 -show

-IMPORT	JSON biçimli bir amass dosyasını içeri aktarır.	amass db -import PATH
-IP	Keşfedilen alan adlarının IP adreslerini de gösterir.	amass db -show -ip -d example.com
-IPV4	Keşfedilen alan adlarının IPv4 adreslerini de gösterir.	amass db -show -ipv4 -d example.com
-IPV6	Keşfedilen alan adlarının IPv6 adreslerini de gösterir.	amass db -show -ipv6 -d example.com
-JSON	JSON biçimli kaydedilecek çıktı dosyasının yolunu tanımlar.	amass db -names -silent -json out.json -d example.com
-LIST	Keşifte kullanılacak veri kaynaklarını listeler.	amass db -list
-NAMES	Sadece keşfi yapılmış alanadlarını getir.	amass db -names -d example.com
-NOCOLOR	Renkli çıktıyı devre dışı bırakır.	amass db -names -nocolor -d example.com
-O	Metin çıktı dosyasının yolunu belirtir.	amass db -names -o out.txt -d example.com
-SHOW	Elde edilen keşif dizini + etki alanları için sonuçları yazdırır.	amass db -show
-SILENT	Yürütme sırasında tüm çıktıları devre dışı bırakır.	amass db -names -silent -json out.json -d example.com
-SRC	Keşfedilen alanların hangi kaynaktan temin edildiğini gösterir.	amass db -show -src -d example.com
-SUMMARY	Yalnızca ASN tablosu özetini yazdırır.	amass db -summary -d example.com

Önceki taramalarınızın tüm ayrıntılarını listelemek için, sadece amass db -show'u çalıştırın,böylece yeni bir taramaya gerek olmadan mevcut sonuçları görebilirsinzi. Belirli bir alan adının ayrıntılarını görmek istiyorsanız, -d seçeneğini eklemeniz yeterlidir:

```
amass db -show -d paypal.com
```

Güzel, temiz, sade bir çıktıyı tercih ederseniz, keşfedilen etki alanlarını/alt etki alanlarını -show yerine -names seçeneğini kullanarak yazdırabilirsiniz.

```
amass db -dir amass4owasp -d owasp.org -enum 1 -show
```

amass4owasp dizininde kayıtlı veritabanında yer alan owasp.org alan adına ait 1 numaralı keşfin sonuçlarını görüntüler.

API anahtarlarını oluşturmak

Amass'ın kullanabileceği birçok veri kaynağı var. Makalenin başında bunların bir listesini vermiştim. Ancak aşağıda listesini görebileceğiniz veri kaynakları API anahtarına ihtiyaç duyarlar.

AlienVault, BinaryEdge, BufferOver, BuiltWith, C99, Censys, Chaos, CIRCL, DNSDB, DNSTable, FacebookCT, GitHub, HackerOne, HackerTarget, NetworksDB, PassiveTotal, RapidDNS, Riddler, SecurityTrails, Shodan, SiteDossier, Spyse, Twitter, Umbrella, URLScan, VirusTotal, WhoisXML, ZETAlytics, Cloudflare

Bu API anahtarlarının çoğu ücretsizdir, ancak ücretli bir API anahtarınız olmadığı sürece çoğu yalnızca sınırlı sonuçlar verir. Ücretsiz olanlar ise hiç olmamasından iyidir. Yukarıdaki hizmetlerin her biri için web sitesini bulmanız, ardından kaydolmanız ve bir API anahtarı almanız gerekecektir. Bu çok zaman alıcı ve sıkıcı bir iştir, ancak iyi keşif fedakarlık olmadan gelmez. Bunu yapabilirsiniz. Tüm API anahtarlarınızı aldıktan sonra, bunları amass yapılandırma dosyasına yapıştırın. Kapsamlı bir örnek yapılandırma dosyası için buraya bakın. Aşağıda bir yapılandırma dosyası içeriği gözüküyor. Bunlardan Paid yazanlar ücretlidir. Örnek dosyadaki API kullanan veri kaynaklarından dilediklerinizi elde edip aşağıdaki gibi ekleyin ve kendi amass config dosyasınızı oluşturun. Daha sonra dosyayı örneğin amassconfig.ini ismiyle kaydedin:

```
# https://passivedns.cn (Contact)
[data_sources.360PassiveDNS]
[data_sources.360PassiveDNS.Credentials]
apikey = sizeozelapikodu

# https://ahrefs.com (Paid)
[data_sources.Ahrefs]
ttl = 4320
[data_sources.Ahrefs.Credentials]
apikey = sizeozelapikodu

# https://otx.alienvault.com (Free)
[data_sources.AlienVault]
[data_sources.AlienVault.Credentials]
apikey =sizeozelapikodu
```

Şimdi, amass kullandığınızda, yapılandırma dosyasını aşağıdaki gibi -config parametresiyle belirtin. Böylece intel ve enum keşiflerinizin sayısı ve kalitesi artacaktır. Diğerlerinden bir adım öne geçebilmek için bunu mutlaka yapmanızı tavsiye ederim.

```
amass enum -d turkiye.gov.tr -config ./amasconfig.ini
```

Çıktı dizini

amass son tarama oturumu ile ilgili günlük ve çıktı dosyalarını varsayılan olarak ~/.config/amass altında tutar. Yeni bir tarama yapıldığında bu dosyalar sıfırlarlanır. log dosyası tarama sürecinin nasıl ilerlediği ve olası hataları kayıt altında tuttuğundan tarama sonunda incelenmelidir. Benzer şekilde tarama çıktısı CSV biçiminde yine bu dizinde depolanır. Her tarama için farklı depo dizini kullanmak faydalı olabilir. Bunun için komuta -dir seçeneğini verebilirsiniz. Aşağıdaki örneği inceleyin:

```
amass intel -asn 47524 -src -ip -dir turksat -config amass-apis.ini
```

Yukarıdaki komut ile ASN (otonom ağ) numarası 47524 olan TURKSAT ağı araştırılarak keşifler turksat dizinine kaydedilecektir.

Referanslar

Amass Projesi Web Sitesi: https://owasp-amass.com/
Amass Kaynak Kodu: https://github.com/OWASP/Amass
Kullanım kılavuzu: https://github.com/OWASP/Amass/blob/master/doc/user_guide.md
Kullanım örnekleri: https://github.com/OWASP/Amass/blob/master/doc/tutorial.md
Haklukes'in kullanım kılavuzu: https://hakluke.medium.com/haklukes-guide-to-amass-how-to-use-amass-more-effectively-for-bug-bounties-7c37570b83f7

Telif Hakları