Amass: Bilgi Toplama Aracı



AMASS

Bir OWASP projesi olan Amass, Açık kaynak istihbaratı (OSINT) alanında kullanılan önemli toollardan birisidir. Temel odağı subdomain (alt alan) keşfi yapmaktır. Özetle Amass, açık kaynak bilgi toplama ve aktif keşif yöntemleri kullanarak saldırı yüzeylerinin (Attack surface) ağ haritasını ve harici varlık keşfini yapmaktadır. Bu işlemleri yaparken çeşitli bilgi toplama teknikleri kullanmaktadır. Bunlar:

*DNS:* Brute forcing, Reverse DNS sweeping, NSEC zone walking, Zone transfers, FQDN alterations/permutations, FQDN Similarity- based Guessing

*Scraping (kazıma):* AbuseIPDB, Ask, AskDNS, Baidu, Bing, DNSDumpster, DuckDuckGo, Gists, HackerOne, HyperStat, IPv4Info, PKey, RapidDNS, Riddler, Searchcode, Searx, SiteDossier, SpyOnWeb, Yahoo

*Sertifikalar:* Active pulls (optional), Censys, CertSpotter, Crtsh, Digitorus, FacebookCT, GoogleCT

*API’ler:* 360PassiveDNS, ARIN, Ahrefs, AlienVault, AnubisDB, BinaryEdge, BGPView, BufferOver, BuiltWith, C99, Chaos, CIRCL, Cloudflare, CommonCrawl, DNSDB, DNSlytics, DNSRepo, Detectify, FOFA, FullHunt, GitHub, GitLab, Greynoise, HackerTarget, Hunter, IntelX, IPdata, IPinfo, LeakIX, Maltiverse, Mnemonic, N45HT, NetworksDB, ONYPHE, PassiveTotal, PentestTools, Quake, RADb, Robtex, SecurityTrails, ShadowServer, Shodan, SonarSearch, Spamhaus, Spyse, Sublist3rAPI, TeamCymru, ThreatBook, ThreatCrowd, ThreatMiner, Twitter, Umbrella, URLScan, VirusTotal, WhoisXMLAPI, ZETAlytics, ZoomEye

***Web Arşivleri:* ArchiveIt, Arquivo, HAW, UKWebArchive, Wayback**

Kurulumu github üzerinden kolayca yapılabilmektedir. Linki; <https://github.com/OWASP/Amass.git> [(https://github.com/OWASP/Amass.git)](https://github.com/OWASP/Amass.git)

Amass kurulumu tamamlandıktan sonra aracın fonksiyonlarını öğrenme kısmına geçilebilir. *“amass –help veya amass”* komutu ile tool kullanımını ve yapılabilecekleri rahatlıkla görebilmekteyiz.



Kullanımı: amass intel |enum|viz|track|db|dns [options(seçenekler)] şeklindedir. Alt komutlarını tanımlamak gerekirse:

*amass intel:* Hedefleri keşfetmede kullanılmaktadır. Alt parametrelerini görmek için “amass intel” komutunu kullanmaktayız. *amass enum:* İncelenecek hedefte numaralandırma ve ağ eşlemesini kolayca gerçekleştirmektedir.. Alt parametrelerini görmek için “amass enum” komutunu kullanmaktayız.

*amass viz:* Hedef hakkında sonuçları görsel anlamda ifade etmeyi sağlamaktadır. Alt parametrelerini görmek için “amass viz” komutunu kullanmaktayız.

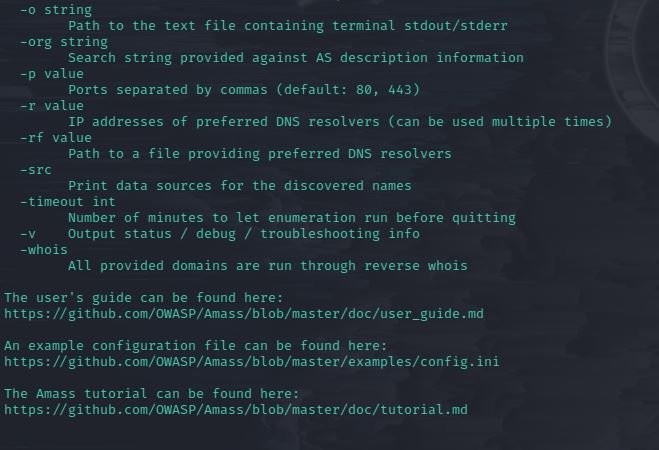
*amass track:* İncelenecek hedefteki numaralandırmalar arasındaki farkları gözlemleme imkanı sağlar. Alt parametrelerini görmek için “amass viz” komutunu kullanmaktayız.

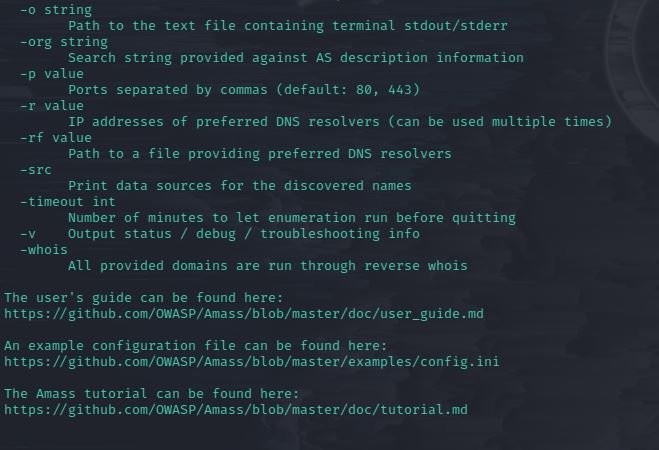
*amass db:* Amass verilerini grafik veritabanına işlemektedir. Alt parametrelerini görmek için “amass viz” komutunu kullanmaktayız.

Sırası ile genel mantığını anlamaya çalışalım ve sık kullanılan parametreleri inceleyelim.

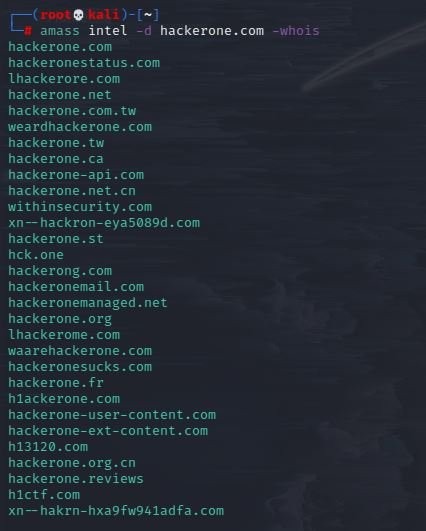
# 1-) Amass İntel

Bu modül, hedef kuruluş hakkında açık kaynak istihbaratı toplamaya yardımcı olur ve hedefle ilgili daha fazla subdomain bulmayı sağlar. Amass intel modülünün alt komutlarına erişmek için terminale “amass intel” yazmak yeterli olacaktır.





Kullanımına örnek olarak “amass intel -d hedef –whois” komutu ile, hedefe ait istihbarat bilgilerini tespit etmek için Whois ve IPv4Info gibi çeşitli bilgi toplama tekniği ve veri kaynaklarını kullanarak bize sonuçlar getirecektir. Buradaki "–d" parametresi etki edeceği host bilgisini, "-whois" parametresi ise ne için bulunduğunu belirtir.

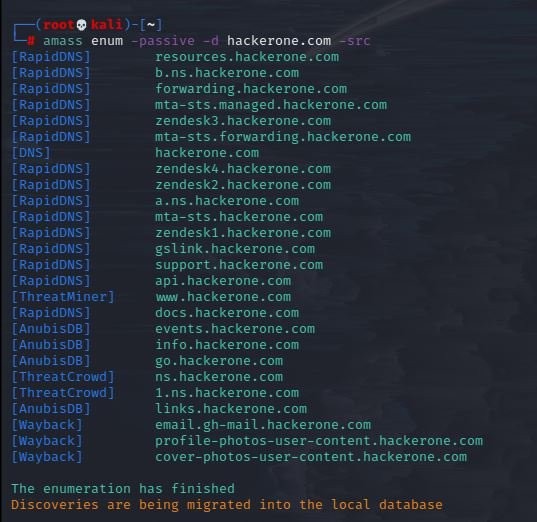


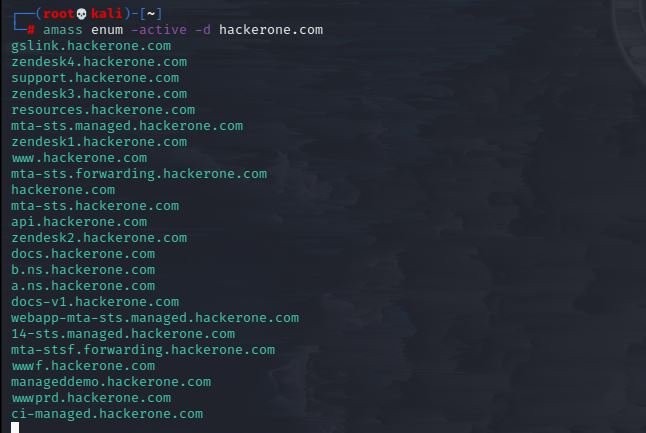
Amass toolunu kullanırken her zaman daha fazla parametre kullanmak ayrıntıyı daha da arttıracaktır. Örnek olarak SSL/TLS sertifikalarını almak için aktif olarak tarayacak olan “-active” parametresi kullanılabilir. Hedef üzerinde aktif bir tarama yapacağından dolayı risklidir, dikkat edilmesi gerekilmektedir.

# 2-) Amass Enum

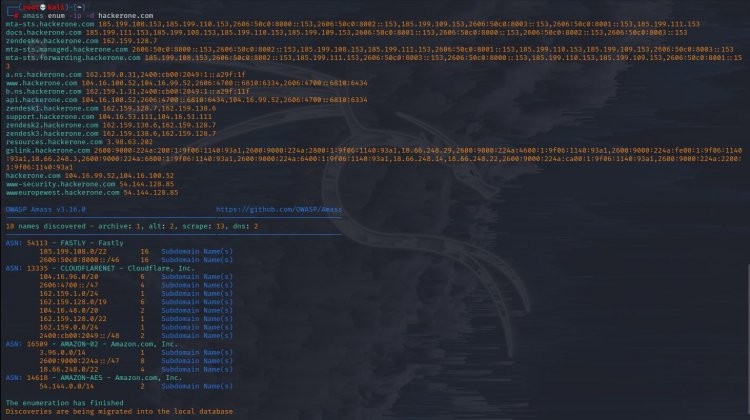
Amass’ ın birçok etkili komutu bu başlığın altında bulunmaktadır. Bu seçenek, hedefin etkisinde kaldığı saldırı yüzeyini tespit etmede hedefin DNS numaralandırmasını ve haritalamasını yapmaktadır. Amass Enum modülünün alt komutlarına erişmek için terminale “amass enum” yazmak yeterli olacaktır.

Kullanıma örnek “amass enum –passive –d hedef –src” ve “amass enum –active –d hedef” komutları ile olarak hedefin subdomainlerini bulmaya çalışalım. Bunu 2 çeşit tarama şekli pasif ve aktif taramadır.





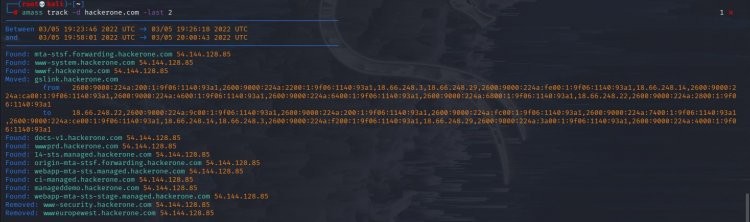
Ek olarak bu bilgileri “amass enum –ip –d hedef” komutunu kullanarak subdomainlere artı olarak IP adreslerini de bulabiliriz.



Bu çıktıda domainleri, subdomainleri, IP bilgilerini, ASN bilgileri ile IP’nin bulunduğu ISP (İnternet Servis Sağlayıcısı) ve ISP’ lerin IP bloklarını tespit edebilmiş olduk. Bu sonuçlar Amass enum‘ un güçlü olma durumunu etkili bir şekilde gözler önüne sermektedir.

# 3-) Amass Track

Hedefe göre numaralandırma sonucuna dayalı sonucu analiz etmeye yardımcı olmaktadır. Örnek basit bir kullanım olarak “amass track – d hedef –last 2” komutu kullanılarak “-last 2” yi hedefe göre karşılaştırma numaralandırmasına dayanarak son 2 numaralandırmayı karşılaştırır.

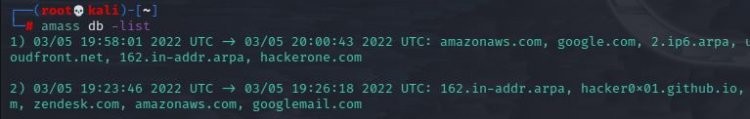


# 4-) Amass Viz

Toplanılan bilgileri farklı şekillerde görselleştirmeye yardımcı olmaktadır. Aynı zamanda daha fazka OSINT analizi için bu verileri Maltego’ ya aktarabilme imkanı sunmaktadır. Örnek olarak kullanılacak komut: “amass viz –d3 –d hedef”

# 5-) Amass DB

Amass grafik veritabanı ile etkileşim kurmak için kullanılan bir komuttur. Örnek olarak Amass üzerinde yapılan arama listesi görülebilir. Kullanılacak komut: “amass db –list”



Spesifik tarama sonuçları olarak belirli bir taramayı görüntülemek için ek olarak “-show” parametresi kullanılır. Kullanılacak komut: “amass db –show –d hedef”

