OWASP amass BENUTZERHANDBUCH

Autor : Özgür Koca, ozgurkoca.com, Juni 2022

Github : https://github.com/enseitankado/owasp-amass-diagrams

OWASP Amass führt eine Netzwerkkartierung von Angriffszielen und die Erkennung externer Assets durch, indem es Open-Source-Informationssammlung und aktive Erkennungstechniken verwendet. Sehen Sie sich hier die Techniken an, die das Tool verwendet, um Subdomains zu finden . Amass , ein OWASP - Projekt, ist eines der wichtigen blueteam- Tools im Bereich Open Source Intelligence (OSINT) . Das Hauptaugenmerk des in der Go -Sprache geschriebenen Tools liegt auf der Intelligenz und Entdeckung von Domainnamen.

Das OWASP Amass-Tool erhält Subdomains durch Scraping von Datenquellen, rekursives Brute-Force, Scannen von Webarchiven, Zulassen/Ändern von Namen und Reverse-DNS-Scannen. Darüber hinaus verwendet Amass während der Auflösung erhaltene IP-Adressen, um zugehörige Netzwerkblöcke und ASNs zu erkennen. Alle Informationen werden dann verwendet, um Karten von Zielnetzwerken zu erstellen. Zu den Forschungs- und Entdeckungstechniken, die Amass verwendet, gehören:

- **Modifikation/Permutation** : Primitive Änderungen an gefundenen Subdomains (dev1 <-> dev2). Wenn es eine Subdomain wie kunde1.domain.com sieht, scannt es auch sequenzielle Subdomains wie kunde2.domain.com.
- **Fuzzy-Tag/String-Suche** : Addition Subtraktion (dev <-> dav). Wenn es eine Subdomain wie dev.domain.com sieht, versucht es, mögliche Subdomains mit einfachen Buchstabenänderungen zu finden.
- **Rekursive Brute Force** : Durchsuchen von APIs und WEB-Archiven. Es sucht nach Subdomains aus Archiven wie wayback.com und archiveit.com. Die von ihm untersuchten

Datenquellen sind unten aufgeführt. Einige davon sind eingeschränkte Dienste, die einen API-Schlüssel benötigen.

- **Aktive Techniken** : Herunterladen von HTTP-TLS/SSL-Zertifikaten. Common Name enthält Subdomain-Informationen.
- **Zonen** : Überwachung von Zonentransfers und Zonenwanderungen (NSEC-Aufzeichnungen).
- **Öffentliche Quellen** : Webarchive, Pastebin, Versionskontrolle und Social-Media-Websites.
- **Certificate Transparancey (CT)-Protokolle** : CT ist ein Framework, mit dem Zertifikate nachverfolgt und überprüft werden können, ob ein Zertifikat sicher oder bösartig ist. Es versucht, mithilfe der für die Domäne definierten Zertifikate zu erkennen.
- **HTTP-CSP-Header (Content Security Policy)** : Wenn Subdomains in den Richtlinien enthalten sind, werden sie hier auf die Whitelist gesetzt, um sie vor CSS-Angriffen zu schützen. Dadurch wird eine Datenquelle für eine Masse in Whitelists erstellt.

Nachfolgend sind die Datenquellen aufgeführt, die Amass für Forschung und Entdeckung verwendet. Sie können den folgenden Befehl ausführen, um die aktuellen Datenquellen und die Verfügbarkeit von amass anzuzeigen.

```
enum-Liste anhäufen
```

Amass kann rund 50 Datenquellen nutzen, einige davon kostenlos, einige mit Testnutzung und einige recht teure Dienste. Sie können Ihren Befehlen den Parameter -src hinzufügen, um die erfolgreichsten Datenquellen zu verfolgen. So behalten Sie den Überblick, welche Quelle wie oft Ergebnisse liefert.

TECHNISCH	DATENQUELLE
APIS	360PassiveDNS, Ahrefs, AnubisDB, BinaryEdge, BufferOver, BuiltWith, C99, Chaos, CIRCL, Cloudflare, DNSDB, DNSRepo, Detectify, FOFA, FullHunt, GitHub, GitLab, Greynoise, HackerTarget, Hunter, IntelX, LeakIX, Maltiverse, MHT45 PassiveTotal, PentestTools , Quake, Shodan, SonarSearch, Spamhaus, Spyse, Sublist3rAPI, ThreatBook, ThreatCrowd, ThreatMiner, Twitter, URLScan, VirusTotal, ZETAlytics, ZoomEye
ZERTIFIKATE	Aktive Pulls (optional), Censys, CertSpotter, Crtsh, Digitorus, FacebookCT, GoogleCT
DNS	Brute Force, Reverse DNS Sweeping, NSEC Zone Walking, Zone Transfers, FQDN-Änderungen/-Permutationen, FQDN Similarity-Based Guessing
ORIENTIERUNG	ARIN, BGPTools, BGPView, IPdata, IPinfo, NetworksDB, RADb, Robtex, ShadowServer, TeamCymru
KRATZEN	AbuseIPDB, Ask, Baidu, Bing, DNSDumpster, DuckDuckGo, Gists, HackerOne, HyperStat, IPv4Info, PKey, RapidDNS, Riddler, Searchcode, Searx, SiteDossier, Yahoo
WEB-ARCHIVE	AlienVault, AskDNS, DNSlytics, ONYPHE, SecurityTrails, SpyOnWeb, Umbrella, WhoisXMLAPI
WHOIS-EINTRÄGE	AlienVault, AskDNS, DNSlytics, ONYPHE, SecurityTrails, SpyOnWeb, Umbrella, WhoisXMLAPI

Amass ist ein sehr umfassendes und fortschrittliches Tool. Das Tool enthält 5 Unterbefehle, intel, enum, viz, track und db. **Das Intel** -Kommando erkundet das Ziel. Nützlich, um einen Startpunkt für das Ziel festzulegen. **enum** ordnet das Ziel zu, um mögliche Angriffspunkte zu identifizieren. **viz** hilft bei einer besseren Analyse, indem es die erzielten Ergebnisse visualisiert. **track** wird verwendet, um Änderungen im Laufe der Zeit auf dem Ziel zu verfolgen und zu vergleichen. amass speichert alle Informationen und Scan-Ergebnisse in einer eigenen Datenbank. Der Unterbefehl **db wird** verwendet, um auf diese Datenbank zuzugreifen und sie abzufragen. Sie können auf die Dokumentseite verweisen, um auf alle Befehle und Optionen von amass zuzugreifen . In diesem Kapitel werde ich nur seine grundlegende Verwendung veranschaulichen.

Sammeln Sie Unterbefehle

- **Amass Intel** : Erkennt Root-Domains (nicht Subdomains), ASNs, führt umgekehrte WHOIS- und DNS-Abfragen durch. Es führt Open-Source-Informationen zur Untersuchung der Zielorganisation durch.
- **amass enum** : Extrahiert und mappt DNS-Einträge offener Systeme unter Verwendung von Subdomains, schnellem Modus (passiv), normalem Modus, DNS-Auflösungs-/Validierungstechniken.
- **amass viz** : Erstellt visuelle Grafiken, gut für die visuelle Inspektion. Unterstützt Maltego. Erstellt ein visuelles Diagramm der gemachten Entdeckungen und Forschungen.
- **amass track** : Ermöglicht historische Vergleiche zwischen Scans und das Anzeigen neuer oder aktualisierter Assets.
- **amass db** : Amass speichert alle aktiven und passiven Entdeckungen in seiner eigenen Datenbank. Der Befehl db wird verwendet, um später auf diese Datensätze zuzugreifen.

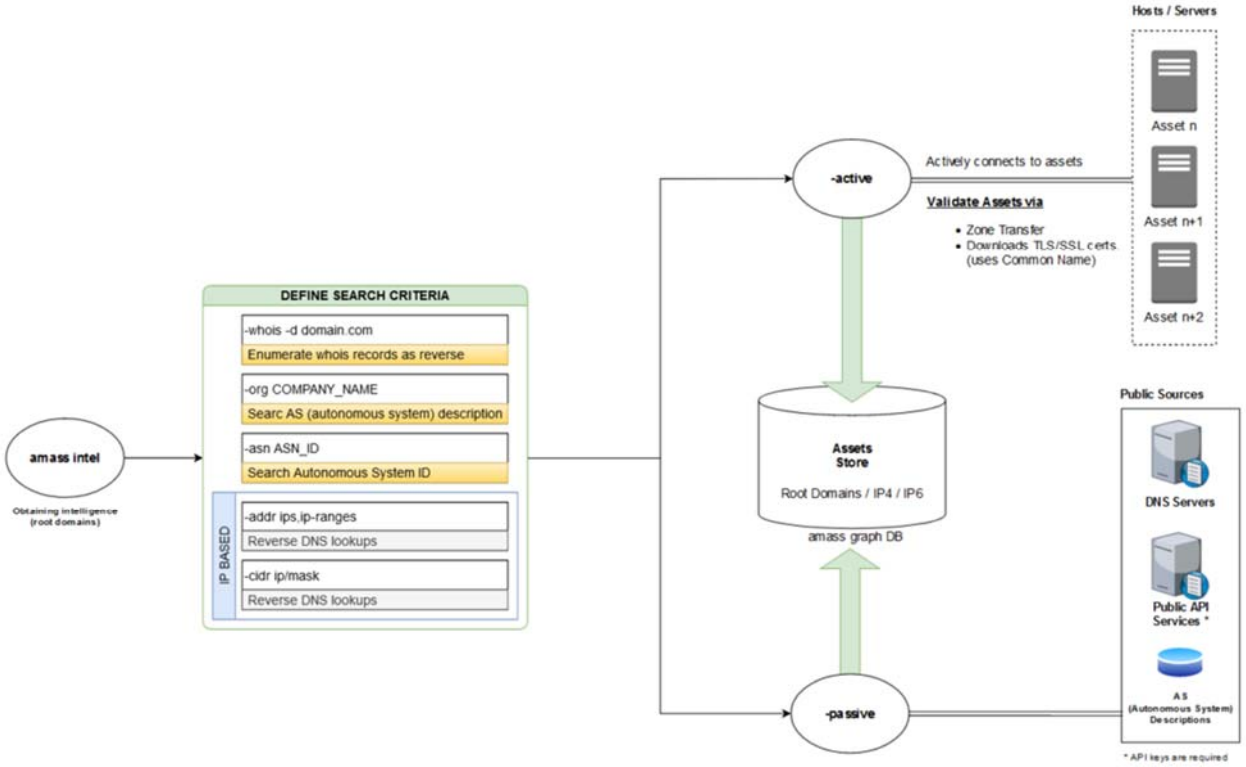
Intel-Befehl

Der Unterbefehl/das Modul Amass Intel kann dabei helfen, Open-Source-Intelligenz über das Unternehmen zu sammeln, und ermöglicht es Ihnen, mehr Stammdomänennamen zu finden, die mit dem Unternehmen verbunden sind. Um die verfügbaren Optionen für diesen Unterbefehl anzuzeigen, geben Sie ihn einfach in das Terminal ein:

```
$ Informationen sammeln
[...]
Verwendung: Amass Intel [Optionen] [-whois -d DOMAIN] [-addr ADDR -asn ASN -
cidr CIDR]
-aktiv
Versuchen Sie, den Namen des Zertifikats abzurufen
-Adr. Wert
IPs und Bereiche (192.168.1.1-254) durch Kommas getrennt
-asn-Wert
Lieferavise durch Komma getrennt (mehrfach verwendbar)
-cidr-Wert
CIDRs durch Komma getrennt (mehrfach verwendbar)
-org-Zeichenfolge
```

```
Suchzeichenfolge, die für AS-Beschreibungsinformationen bereitgestellt wird
-Wer ist
Alle bereitgestellten Domains laufen über Reverse Whois
[...]
```

An dieser Stelle ist anzumerken, dass ein weiterer großer Vorteil von Amass darin besteht, dass alle Unterbefehle versuchen, die Konsistenz der Argumente aufrechtzuerhalten. In den folgenden Abschnitten sind die Parameter der Unterbefehle enthalten, Sie können sehen, dass die meisten von ihnen gemeinsam verwendet werden. Das folgende Diagramm zeigt im Wesentlichen die Arbeitslogik von amass intel.



Standardmäßig verwendet dieser Unterbefehl eine Reihe von Techniken zum Sammeln von Informationen und Datenquellen wie WHOIS und IPv4Info, um Organisationsinformationen und übergeordnete Domänen zu erhalten, sofern dies nicht ausdrücklich in der Konfigurationsdatei von Amass deaktiviert ist. Eine Beispiel-Amass-Konfigurationsdatei ist im [GitHub-Repository verfügbar.]

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

Sie können einige der oben genannten Ergebnisse auch bestätigen, indem Sie die Datenquellen manuell durchsuchen. Im Screenshot unten haben wir eine umgekehrte Whois-Suche nach „OWASP Foundation“ durchgeführt und ViewDNS (ebenfalls Teil der Datenquellen von Amass) nach ähnlichen Domains gefragt:

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

Wenn Sie mit Amass Intel suchen, können Sie es immer mit mehr Konfigurationsoptionen ausführen, zum Beispiel können Sie die Zonenübertragung mit dem Argument --active versuchen und es mit dem relevanten Server verbinden, um die SSL/TLS-Zertifikate zum Extrahieren der Informationen zu erhalten. Stellen Sie einfach sicher, dass Sie berechtigt sind, aktive Suchen nach dem Ziel durchzuführen, bevor Sie dies tun.

An dieser Stelle ist anzumerken, dass einige Konfigurations-Flags mit anderen nicht funktionieren, in diesem Fall wird Amass sie ignorieren.

Die Ergebnisse von Amass sind aus verschiedenen Gründen möglicherweise nicht immer genau, beispielsweise sind die von Amass verwendeten Datenquellen möglicherweise nicht konsistent oder aktuell. Amass versucht, die Informationen mithilfe von DNS-Abfragen weiter zu validieren. Während Amass gute Arbeit leistet, sollten Benutzer dennoch mehr Validierungsprüfungen für Ergebnisse durchführen, die für das Ziel nicht relevant erscheinen. Dies kann mit einer Vielzahl von Methoden erreicht werden, wie z.

- Verwenden Sie Dienstprogramme (z. B. dig, nslookup), um Domänen aufzulösen.
- Führen Sie WHOIS-Suchen durch, um institutionelle Details zu überprüfen.
- Verwenden Sie Suchergebnisse wie Hauptdomänen in Suchmaschinen.

```
amass intel -org TÜRKEI
```

Gibt die ASN-IDs zurück, die sich auf das Wort Türkei beziehen. Diese Art der Zeichenfolgensuche liefert oft nicht genügend Ergebnisse. Sie können auch den Schalter -active hinzufügen, wenn Sie möchten, dass die Suche auch mit aktiven Methoden durchgeführt wird. Der

obige Befehl sucht in den ASN-Beschreibungen nach Türkei und gibt die zugehörigen ASNs zurück.

Der Organisationsschlüssel sucht nach ASN-IDs (autonomes System), die dem angegebenen Ausdruck zugeordnet sind. Die mit dem Parameter -org angegebene Zeichenfolge wird in AS-Datensätzen gesucht und ihre ASN-ID wird gefunden. ASN-ID ist die von der Internet Assigned Numbers Authority (IANA) vergebene autonome Systemnummer, die durch eine weltweit eindeutige 16-stellige Identifikationsnummer repräsentiert wird. Ein AS (Autonomes System) bezieht sich auf ein großes Netzwerk oder eine Gruppe von Netzwerken mit einer einzigen Routing-Richtlinie (rfc1930). Identifiziert sie in der Lieferavis-ID. Beispielsweise lautet die ASN-Nummer des Netzwerks von TTNET 9121, die von CloudFlare 13335, die von ULAKNET 8517 und die von Amazon 16509. Große Router nutzen diese ASN-Nummern, wenn das Routing zwischen Netzwerken erfolgen muss.

Versuchen wir nun, die Domänennamen in einer von uns gefundenen ASN zu finden. Sehen Sie sich den folgenden Befehl an.

```
amass intel -active -src -ip -asn 8517 -p 80.443
```

Es wird eine Entdeckung unter Verwendung aktiver Techniken (-aktiv) auf den Ports 80 und 443 von Domänen im autonomen Netzwerk (ULAKNET) mit der ASN-Nummer 8517 machen. Es verwendet TLS/SSL-Zertifikate für die aktive Erkennung. amass zieht das SSL-Zertifikat, das sich mit allen IP-Adressen der angegebenen ASN verbindet, und listet die Domain auf, der das SSL-Zertifikat zugeordnet ist. Es zeigt auch die Quell- (-src) und IP-Adressen (-ip) der gefundenen Domänen an.

```
amass intel -active -ip -src -cidr 193.140.28.0/24 -p 80.443
```

Ein Zeichenfolgenbereich wird mit dem Parameter -cidr deklariert. Die Zahl 24 stellt die Netzmaske dar und entspricht 255.255.255.0. amass sucht und entdeckt verschiedene Quellen für IP-Adressen zwischen 193.140.28.1 und 193.140.28.254, erkennt und listet die an diese IPs gerichteten Domainnamen auf. Außerdem erfolgt die aktive Erkennung mithilfe von TLS/SSL-Zertifikaten für die Ports 80 und 443. Es stellt eine Verbindung zu jeder IP-Adresse her, ruft SSL-Zertifikate ab und listet die im Zertifikat erwähnten Domänennamen auf.

```
amass intel -active -ip -src -cidr 74.6.0.6/16 -addr 74.6.231.20-21 -p 80.8080
```

Es scannt Computer im Netzwerk 74.6.0.6/16 mit aktiven Techniken. Es listet die IP-Adresse und die Quelle der gefundenen Domänen auf. Es führt eine umgekehrte DNS-Abfrage auf Computern im Bereich 74.6.231.20-21 durch.

```
Sammeln Sie Informationen -whois -d yahoo.com
```

Es versucht, Domänennamen zu finden, indem es die WHOIS-Datensätze der angegebenen Domäne (-d) oder Domänenliste (-df) rückwärts durchsucht. In diesem Beispiel greift amass auf die WHOIS-Einträge von yahoo.com zu und versucht, die Root-Domains anderer Organisationen zu finden, die möglicherweise mit diesen WHOIS-Einträgen identisch sind. Es ist nützlich, um andere Domains zu finden, die zu einer Organisation/einem Unternehmen gehören, aber WHOIS-

Einträge enthalten möglicherweise nicht immer genaue Informationen oder werden vertraulich behandelt.

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

Dieser Befehl sucht nach anderen Domänen mit denselben WHOIS-Einträgen im autonomen ULAKNET-Netzwerk mit der ASN-ID 8517.

Nachfolgend finden Sie eine Tabelle, die die Optionen und Anwendungsbereiche des Intel-Befehls zeigt.

AUSWAHL	ERLÄUTERUNG	PROBE
-AKTIV	Es verwendet aktive Methoden. Zone versucht zu übertragen, stellt eine Verbindung zum Zielserver her, um SSL/TLS-Zertifikate zu erhalten.	amass intel -active -addr 192.168.2.1-64 -p 80.443.8080
-ADR	Gibt IP-Bereiche an. Bereiche werden durch Kommas getrennt.	192.168.2.1-64,192.168.3.10-254
- ASN	Meldet ASN-ID. Die ASN-ID ist eine eindeutige Nummer, die großen Computernetzwerken von IANNA zugewiesen wird.	Sammeln Sie Intel -asn 13374,14618
-CIDR	Definiert ein Netzwerk. Die Zahl nach dem Schrägstrich definiert die Netzmaske.	Sammeln Sie Intel-Cidr 104.154.0.0/15
-KONFIG	Gibt den Speicherort der Scankonfigurationsdatei an.	amass intel -config config.ini
-D	Feldnamen durch Kommas getrennt.	amass intel -whois -d example.com
-DF	Es speist Root-Domains aus einer Datei.	amass intel -whois -df domains.txt
IST	Gibt den Pfad zu dem Verzeichnis an, das die Datenbank enthält, in der die Scanergebnisse gespeichert werden.	amass intel -dir PATH -cidr 104.154.0.0/15
-EF	Der Pfad zu der Datei mit einer Liste von Datenquellen, die bei der Recherche nicht verwendet werden.	amass intel -whois -ef exclude.txt -d example.com
-AUSSCHLIEßEN	Liste der Datenquellen, die beim Scannen nicht verwendet werden. Sie wird durch ein Komma getrennt angegeben.	amass intel -whois -exclude crtsh -d example.com

-WENN	Pfad zur Datei mit einer Liste von Datenquellen, die zum Scannen verwendet werden sollen.	amass intel -whois -if include.txt -d example.com
-ENTHALTEN	Liste der zum Scannen zu verwendenden Datenquellen. Es wird durch Kommas getrennt geschrieben.	amass intel -whois -include crtsh -d example.com
-SEIL	Es zeigt auch die IP-Adressen der entdeckten Domains.	amass intel -ip -whois -d example.com
-IPV4	Es zeigt auch die IPv4-Adressen der erkannten Domänen.	amass intel -ipv4 -whois -d example.com
-IPV6	Außerdem werden die IPv6-Adressen der erkannten Domänen angezeigt.	amass intel -ipv6 -whois -d example.com
-AUFFÜHREN	Listet die Datenquellen auf, die bei der Erkennung verwendet werden sollen.	Sammeln Sie eine Intel-Liste
-PROTOKOLL	Meldet den Pfad zur Protokolldatei, in der Fehler protokolliert werden.	amass intel -log amass.log -whois -d example.com
-MAX-DNS-ABFRAGEN	Maximale Anzahl gleichzeitiger DNS-Abfragen.	amass intel -max-dns-queries 200 -whois -d example.com
-ER	Der Pfad zu der Datei, in der die Ausgabe gespeichert wird.	amass intel -o out.txt -whois -d example.com
-ORGAN	Zeichenfolgenausdruck, nach dem in der AS-Anweisung gesucht werden soll.	amass intel -org Facebook
-P	Durch Kommas getrennte Portnummern.	Sammeln Sie Intel -Cidr 104.154.0.0/15 -p 443.8080
-R	Deklariert DNS-Server, die während der Erkennung verwendet werden sollen.	amass intel -r 8.8.8.8,1.1.1.1 -whois -d example.com
-RF	Gibt den Pfad der Datei an, die die Liste der DNS-Server enthält, die während der Erkennung verwendet werden sollen.	amass intel -rf data/resolvers.txt -whois -d example.com
-QUELLE	Gibt die Quelle an, aus der die entdeckten Felder bezogen wurden.	amass intel -src -whois -d example.com
-AUSZEIT	Timeout-Zeitraum, der während der Erkennung zu berücksichtigen ist.	amass intel -timeout 30 -d example.com
-WER IST	WHOIS-Informationen suchen nach anderen ähnlichen Domains.	amass intel -whois -d example.com

amass enum-Befehl

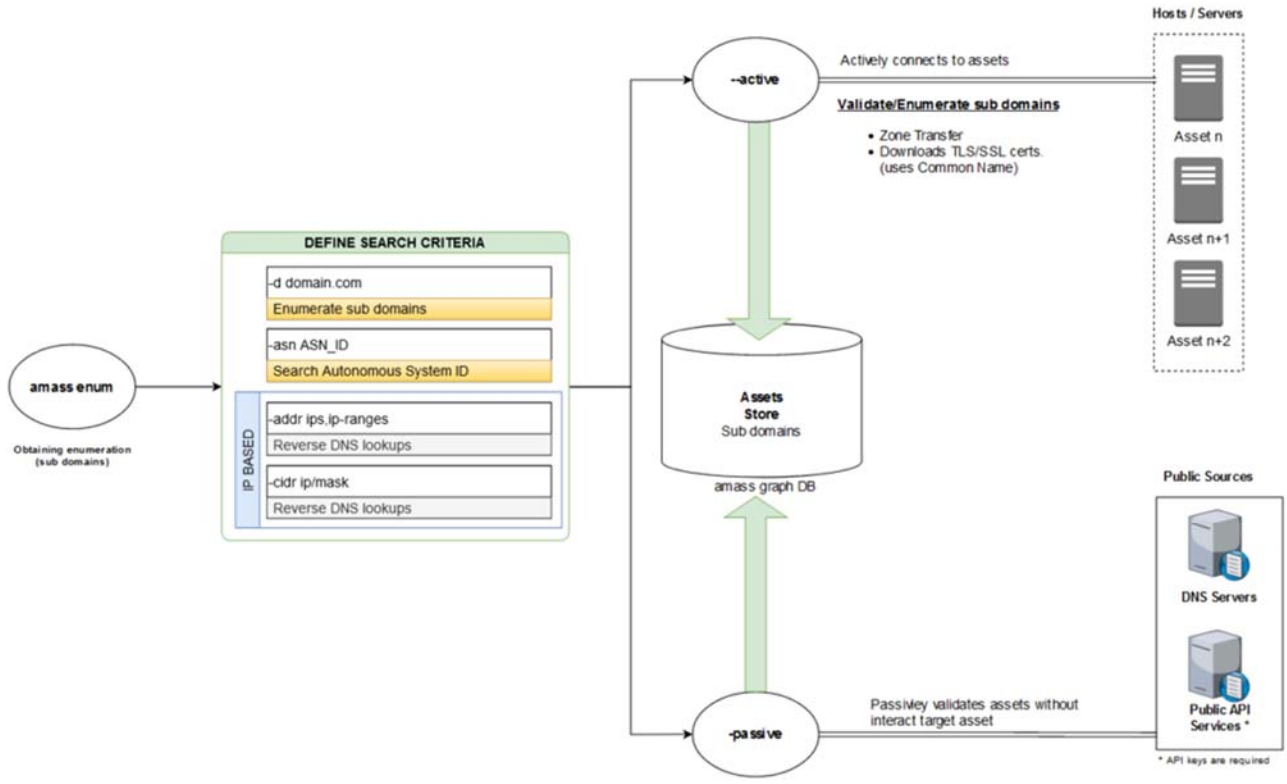
Amass enum kann in einem passiven oder aktiven Modus ausgeführt werden. Der passive Modus ist viel schneller, aber Amass validiert DNS-Informationen nicht durch Auflösen von Subdomains. Sie können es mit dem Flag „-passive“ passiv ausführen und können viele Techniken oder Konfigurationen wie DNS-Auflösung und -Validierung nicht aktivieren. Manchmal ist es notwendig, den passiven Modus anstelle des aktiven Modus zu wählen, zum Beispiel:

- Da Sie den Zielbereich ständig auf Änderungen überwachen müssen oder weil Sie an einer Phishing-Interaktion arbeiten und nach Unterdomänen suchen, müssen Sie alle möglichen Unterdomänen kennen, die verwendet wurden und möglicherweise in Zukunft wiederverwendet werden.
- Möglicherweise müssen Sie DNS-Informationen zu einem späteren Zeitpunkt überprüfen und Ergebnisse schnell spoolen.
- Aufgrund der Einschränkungen oder Anforderungen eines Sicherheitseinsatzes müssen Sie möglicherweise nur eine passive Informationserfassung durchführen.

Um die verfügbaren Optionen für diesen Unterbefehl anzuzeigen, geben Sie ihn einfach in das Terminal ein:

```
Verwendung: amass enum [Optionen] -d DOMÄNE

-aktiv
Versuchen Sie, Zonenübertragungen und Zertifikatsnamenszugriffe durchzuführen
-Adr. Wert
IPs und Bereiche (192.168.1.1-254) durch Kommas getrennt
-d Wert
Domainnamen durch Komma getrennt (mehrfach verwendbar)
-cidr-Wert
CIDRs durch Komma getrennt (mehrfach verwendbar)
-asn-Wert
Lieferavise durch Komma getrennt (mehrfach verwendbar)
```



Im folgenden Beispiel suchen wir passiv nach Subdomains auf Owasp.org und bitten Amass, die Datenquellen anzuzeigen, in denen es jede Subdomain findet:

```
$ 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
[...]
Abfrage von VirusTotal nach owasp.org-Subdomains
Abfragen von Yahoo nach owasp.org-Subdomains
[...]
```

Dieser Unterbefehl führt während der Prüfung eine DNS-Erkennung und Netzwerkzuordnung durch. Es ist an dieser Stelle erwähnenswert, dass Amass enum alle Subdomains identifiziert, obwohl der Amass Intel-Befehl hilft, IP-Bereiche, ASNs und Hauptdomains zu sammeln, die einer Organisation gehören.

Die Verwendung von Amass im aktiven Konfigurationsmodus bedeutet, dass Sie genauere Ergebnisse erhalten und mehr Assets entdeckt werden können, da Sie alle DNS-Erkennungstechniken aktivieren können. Bei aktiviertem Konfigurationsmodus sucht es nach Subdomains von Zertifikatdomains (z. B. Common Name) , indem es Zonentransfers und Port-Scans von SSL/TLS-Diensten durchführt .

kann im Allgemeinen als aktiv betrachtet werden, da er Subdomain Brute-Forcing auf mehrere Arten durchführt (Wortliste, Masken usw.) mit aktiviertem „-active“-Flag . Alle Ergebnisse werden von Amass unter Verwendung der standardmäßigen oder angegebenen Analysatoren validiert:

Alle folgenden Einstellungen beziehen sich auf diesen Unterbefehl. Zur Konfiguration stehen folgende Flags zur Verfügung:

Auswahl	***Erläuterung***	***Probe***
-aktiv	Es verwendet aktive Methoden. Zone versucht zu übertragen, stellt eine Verbindung zum Zielserver her, um SSL/TLS-Zertifikate zu erhalten.	amass enum -active -d example.com -p 80.443.8080
-aw	Gibt den Pfad der alternativen Word-Datei an, um Subdomain-Alternativen zu generieren.	amass enum -aw PATH -d example.com
-bl	Meldet eine schwarze Liste von Subdomains, die nicht entdeckt werden.	amass enum -bl blah.example.com -d example.com
-blf	Gibt den Pfad der Datei mit der Liste der Subdomains auf der schwarzen Liste an.	amass enum -blf data/blacklist.txt -d example.com
-roh	Verwendet Brute Force bei der Erkundung von Subdomains.	amass enum -brute -d example.com
-konfig	Gibt den Pfad zur INI-Konfigurationsdatei an.	amass enum -config config.ini
-D	Feldnamen durch Kommas getrennt.	amass enum -d example.com

-df	Es speist Root-Domains aus einer Datei.	amass enum -df domains.txt
ist	Gibt den Pfad zu dem Verzeichnis an, das die Datenbank enthält, in der die Scanergebnisse gespeichert werden.	amass enum -dir PATH -d example.com
-ef	Der Pfad zu der Datei mit einer Liste von Datenquellen, die bei der Recherche nicht verwendet werden.	amass enum -ef exclude.txt -d example.com
-ausschließen	Liste der Datenquellen, die beim Scannen nicht verwendet werden. Sie wird durch ein Komma getrennt angegeben.	amass enum -ef exclude.txt -d example.com
-wenn	Pfad zur Datei mit einer Liste von Datenquellen, die zum Scannen verwendet werden sollen.	amass enum -ef exclude.txt -d example.com
-enthalten	Liste der zum Scannen zu verwendenden Datenquellen. Es wird durch Kommas getrennt geschrieben.	amass enum -include crtsh -d example.com
-Seil	Es zeigt auch die IP-Adressen der entdeckten Domains.	amass enum -ip -d example.com
-ipv4	Es zeigt auch die IPv4-Adressen der erkannten Domänen.	amass enum -ip -d example.com
-ipv6	Außerdem werden die IPv6-Adressen der erkannten Domänen angezeigt.	amass enum -ip -d example.com
-json	Definiert den Pfad der zu speichernden Ausgabedatei im JSON-Format.	amass enum -json out.json -d example.com
-aufführen	Listet die Datenquellen auf, die bei der Erkennung verwendet werden sollen.	enum-Liste anhäufen
-Protokoll	Meldet den Pfad zur Protokolldatei, in der Fehler protokolliert werden.	amass enum -log amass.log -d example.com
-max-dns-Abfragen	Maximale Anzahl gleichzeitiger DNS-Abfragen.	amass enum -max-dns-queries 200 -d example.com
-dns-qps	Maximale Anzahl von DNS-Abfragen pro Sekunde über alle Domain-Resolver (DNS-Server).	amass enum -dns-qps 200 -d example.com
-rqps	Maximale Anzahl von DNS-Abfragen pro Sekunde für jeden nicht vertrauenswürdigen Resolver.	amass enum -dns-qps 200 -d example.com
-trqps	Maximale Anzahl von DNS-Abfragen pro Sekunde für jeden vertrauenswürdigen Resolver	amass enum -trqps 20 -d example.com
-min-für-rekursiv	Subdomain-Labels vor rekursivem Brute-Forcing gesehen (Standard: 1)	amass enum -brute -min-for-recursive 3 -d example.com
-maximale Tiefe	Maximale Anzahl von Subdomain-Tags für Brute Force	amass enum -brute -max-depth 3 -d example.com
-nf	Pfad zu einer Datei, die bereits bekannte Subdomains bereitstellt (aus anderen Tools/Quellen)	amass enum -nf names.txt -d example.com
-Noalts	Deaktiviert die Generierung alternativer Subdomains.	amass enum -noalts -d example.com

-norekursiv	Deaktiviert rekursive Brute-Force.	amass enum -brute -norecursive -d example.com
-Er	Gibt den Pfad zur Textausgabedatei an.	amass enum -o out.txt -d example.com
-oA	Pfadpräfix, das zum Benennen aller Ausgabedateien verwendet wird.	amass enum -oA amass_scan -d example.com
-passiv	Es führt eine vollständig passive Ausführung durch.	amass enum --passive -d example.com
-p	Durch Kommas getrennte Portnummern.	amass enum -d example.com -p 443.8080
-r	Deklariert DNS-Server, die während der Erkennung verwendet werden sollen.	amass enum -d example.com -p 443.8080
-en	IP-Adressen vertrauenswürdiger DNS-Resolver (mehrfach verwendbar)	amass enum -en 8.8.8.8,1.1.1.1 -d example.com
-rf	Gibt den Pfad der Datei an, die die Liste der DNS-Server enthält, die während der Erkennung verwendet werden sollen.	amass enum -en 8.8.8.8,1.1.1.1 -d example.com
-trf	Gibt den Pfad zu einer Datei an, die vertrauenswürdige DNS-Resolver bereitstellt.	amass enum -trf data/trusted.txt -d example.com
-Quelle	Gibt die Quelle an, aus der die entdeckten Felder bezogen wurden.	amass enum -src -d example.com
-Auszeit	Timeout-Zeitraum, der während der Erkennung zu berücksichtigen ist.	amass enum -timeout 30 -d example.com
-w	Meldet den Pfad einer anderen Wortlistendatei.	amass enum -brute -w wordlist.txt -d example.com

Die häufigste Verwendung des Enum-Befehls ist wie folgt. Nachdem dieser Befehl gegeben wurde, beginnt amass damit, die Subdomains des Domainnamens meb.gov.tr aus dem Internet zu durchsuchen. Es fragt alle möglichen Datenquellen ab und gibt einen Stapel von Subdomains zurück.

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

Bei diesem Scan wird ein (-passiver) Scan ohne DNS-Auflösung durchgeführt. Angenommen, passive-config.ini enthält eine Liste passiver Informationsressourcen und API-Schlüssel. Die Option -passive gibt schneller, aber weniger Ergebnisse zurück als -active.

Durch die Verwendung des Parameters -v können Sie den Detaillierungsgrad der amass.log-Datei erhöhen und die Funktionen von amass während der Anwendung besser verstehen. Es ermöglicht Ihnen, Datenquellen zu erkennen, die nicht richtig funktionieren, Dienste zu sehen, die Ihre IP-Adresse blockieren, und DNS-Resolver, die nicht richtig funktionieren.

Track-Befehl anhäufen

Um die Angriffsfläche eines Ziels zu überwachen, zeigt es die Unterschiede zwischen der Aufklärung desselben Ziels bzw. derselben Ziele. Dieser Unterbefehl nutzt nur „output_directory“ und die Einstellungen der entfernten Datenbank, die in der Konfigurationsdatei angegeben sind.

Um die verfügbaren Optionen für diesen Unterbefehl anzuzeigen, geben Sie ihn einfach in das Terminal ein:

```
Verwendung: amass track [Optionen] -d Domain
-d Wert
Domainnamen durch Komma getrennt (mehrfach verwendbar)
-Geschichte
Zeigen Sie den Unterschied zwischen allen Aufzählungspaaren
-letzte int
Die Anzahl der letzten Aufzählungen, die in die Nachverfolgung aufgenommen
werden sollen
```

Auswahl	***Erläuterung***	***Probe***
-konfig	Gibt den Pfad zur INI-Konfigurationsdatei an.	amass track -config config.ini
-D	Feldnamen durch Kommas getrennt.	amass track -d example.com
-df	Es speist Root-Domains aus einer Datei.	amass track -df domains.txt
ist	Gibt den Pfad zu dem Verzeichnis an, das die Datenbank enthält, in der die Scan-Ergebnisse gespeichert werden.	amass track -df domains.txt
-Geschichte	Es zeigt die Unterschiede zwischen den Entdeckungen.	Track-Geschichte anhäufen
-letzte	Die Anzahl der jüngsten Entdeckungen, die in die Nachverfolgung aufgenommen werden sollen.	Sammelspur -letzte 2
-seit	Alle Aufzählungen vor dem angegebenen Datum ausschließen (Format: 01/02 15:04:05 2006 MST)	Track sammeln -seit DATE

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

Der obige Befehl vergleicht die letzten beiden Scans der Domain yahoo.com.

amass viz Befehl

Erstellt anhand der gesammelten Informationen visuelle Netzwerkdiagramme. Diese Visualisierung ist besonders nützlich zum Interpretieren von Beziehungen zwischen Entitäten in großen Scans, die umfassende Ergebnisse zurückgeben. Dieser Unterbefehl nutzt nur das 'output_directory' und die Einstellungen der entfernten Grafikdatenbank aus der Konfigurationsdatei.

Für die Visualisierung erstellte Dateien werden standardmäßig im aktuellen Arbeitsverzeichnis erstellt. Hier sind die Schalter, die verwendet werden können, um DNS- und Infrastrukturergebnisse als Netzwerkdiagramme auszugeben:

Auswahl	***Erläuterung***	***Probe***

-konfig	Gibt den Pfad zur INI-Konfigurationsdatei an.	amass viz -config config.ini -d3
-D	Feldnamen durch Kommas getrennt.	amass viz -d3 -d example.com
-d3	Generiert D3.js v4-formatierte HTML-Simulationsdatei.	amass viz -d3 -d example.com
-df	Definiert den Pfad zu der Datei, die die Stammdomänen enthält.	amass viz -d3 -df domains.txt
ist	Definiert den Pfad zu dem Verzeichnis, das die Graph-Datenbank enthält.	amass viz -d3 -dir PATH -d example.com
-enum	Scan-Ergebnisse identifizieren eine Entdeckung anhand ihrer Indexnummer aus der Datenbank.	amass viz -enum 1 -d3 -d example.com
-Er	Definiert den Pfad zu dem Verzeichnis, in dem die Ausgabedateien gespeichert werden.	amass viz -d3 -o OUTPATH -d example.com
-oA	Definiert ein Präfix für Ausgabedateien.	amass viz -d3 -oA example -d example.com
-gexf	Gibt im Graph Exchange XML Format (GEXF) formatiert aus.	amass viz -gexf -d example.com
-Grafik	Graphistry gibt eine JSON-formatierte Ausgabe zurück.	amass viz -graphistry -d example.com
-Maltego	Gibt die mit Maltego Graph Table formatierte CSV-Datei aus.	amass viz -maltego -d example.com

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

Der obige Befehl zeigt alle Ergebnisse für die Domain yahoo.com in einer HTML-formatierten Datei mit einem assoziativen Diagramm an. Das Diagramm wird mit der d3-Javascript-Bibliothek erstellt . Mit der Option -o wird die Ausgabe im Yahoo-Verzeichnis gespeichert. Der vizz-Befehl kann auch in den Formaten Maltego, XML und JSON ausgegeben werden.

amass db-Befehl

Es ist ein Befehl, mit dem Sie die Erkennungsdaten für jeden durchgeführten Scan anzeigen können. Führt die Anzeige und Verarbeitung der Datenbank durch. Dieser Unterbefehl nutzt nur die Einstellungen für „output_directory“ und entfernte Datenbanken aus der Konfigurationsdatei. Nutzungsmöglichkeiten für die Interaktion mit Explorationsergebnissen in der Datenbank sind:

AUSWAHL	ERLÄUTERUNG	PROBE
-KONFIG	Gibt den Pfad zur INI-Konfigurationsdatei an.	amass db -config config.ini
-D	Feldnamen durch Kommas getrennt.	amass db -d example.com
-DF	Es speist Root-Domains aus einer Datei.	amass db -df domains.txt
IST	Gibt den Pfad zum Datenbankverzeichnis mit den Scanergebnissen an.	amass db -dir PATH

-ENUM	Ruft Ermittlungsinformationen über eine Indexfolgenummer aus der Liste ab.	amass db -enum 1 -show
-IMPORTIEREN	Importiert eine Amass-Datei im JSON-Format.	amass db -import PATH
-SEIL	Es zeigt auch die IP-Adressen der entdeckten Domains.	amass db -show -ip -d example.com
-IPV4	Es zeigt auch die IPv4-Adressen der erkannten Domänen.	amass db -show -ipv4 -d example.com
-IPV6	Außerdem werden die IPv6-Adressen der erkannten Domänen angezeigt.	amass db -show -ipv6 -d example.com
-JSON	Definiert den Pfad der zu speichernden Ausgabedatei im JSON-Format.	amass db -names -silent -json out.json -d example.com
-AUFFÜHREN	Listet die Datenquellen auf, die bei der Erkennung verwendet werden sollen.	amass db -list
-NAMEN	Bringen Sie nur entdeckte Domänen.	amass db -names -d example.com
-KEINE FARBE	Deaktiviert die Farbausgabe.	amass db -names -nocolor -d example.com
-ER	Gibt den Pfad zur Textausgabedatei an.	amass db -names -o out.txt -d example.com
-SHOW	Druckt die Ergebnisse für das resultierende Discovery-Verzeichnis + Domänen.	amass db -show
-LEISE	Deaktiviert alle Ausgaben während der Ausführung.	amass db -names -silent -json out.json -d example.com
-QUELLE	Gibt die Quelle an, aus der die entdeckten Felder bezogen wurden.	amass db -show -src -d example.com
-ZUSAMMENFASSUNG	Druckt nur die Zusammenfassung der ASN-Tabelle.	amass db -summary -d example.com

Um alle Details Ihrer vorherigen Scans aufzulisten, führen Sie einfach amass db -show aus , damit Sie die aktuellen Ergebnisse sehen können, ohne dass ein neuer Scan erforderlich ist. Wenn Sie die Details einer bestimmten Domain sehen möchten, fügen Sie einfach die Option -d hinzu:

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

Wenn Sie eine schöne, saubere und einfache Ausgabe bevorzugen, können Sie die gefundenen Domains/Subdomains mit der Option -names anstelle von -show drucken.

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

Zeigt die Ergebnisse der Entdeckung Nr. 1 des Domänennamens owasp.org in der im amass4owasp-Verzeichnis registrierten Datenbank an.

Generieren von API-Schlüsseln

Es gibt viele Datenquellen, die Amass verwenden kann. Ich habe eine Liste von ihnen am Anfang des Artikels gegeben. Die unten aufgeführten Datenquellen benötigen jedoch den API-Schlüssel.

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

Die meisten dieser API-Schlüssel sind kostenlos, aber die meisten liefern nur begrenzte Ergebnisse, es sei denn, Sie haben einen kostenpflichtigen API-Schlüssel. Kostenlose sind besser als nichts. Sie müssen die Website für jeden der oben genannten Dienste finden, sich dann anmelden und einen API-Schlüssel erhalten. Dies ist eine sehr zeitaufwändige und mühsame Aufgabe, aber eine gute Entdeckung kommt nicht ohne Opfer. Du kannst das. Sobald Sie alle Ihre API-Schlüssel haben, fügen Sie sie in die Amass-Konfigurationsdatei ein. Hier finden Sie eine umfassende Beispielkonfigurationsdatei . Unten ist der Inhalt einer Konfigurationsdatei. Wer Paid schreibt, wird bezahlt. Rufen Sie eine der Datenquellen über die API in der Beispieldatei ab, fügen Sie sie wie folgt hinzu und erstellen Sie Ihre eigene Amass-Konfigurationsdatei. Speichern Sie dann die Datei beispielsweise unter dem Namen amassconfig.ini:

```
# https://passivedns.cn (Kontakt)
[data_sources.360PassiveDNS]
[data_ sources.360PassiveDNS.Credentials ]
apikey = sizeozelapicode

# https://ahrefs.com (kostenpflichtig)
[data_ sources.Ahrefs ]
ttl = 4320
[data_ sources.Ahrefs.Credentials ]
apikey = sizeozelapicode

# https://otx.alienvault.com (kostenlos)
[data_ sources.AlienVault ]
[data_ sources.AlienVault.Credentials ]
apikey =sizeozelapicode
```

Wenn Sie jetzt amass verwenden, geben Sie die Konfigurationsdatei mit dem Parameter -config wie folgt an. Dies erhöht die Anzahl und Qualität Ihrer Intel- und Enum-Entdeckungen. Ich empfehle Ihnen dringend, dies zu tun, um den anderen einen Schritt voraus zu sein.

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

Ausgabe Verzeichnis

amass speichert Protokoll- und Ausgabedateien für die letzte Scansitzung standardmäßig unter ~/.config/amass. Diese Dateien werden zurückgesetzt, wenn ein neuer Scan durchgeführt wird. Die Protokolldatei sollte am Ende des Scans überprüft werden, da sie den Fortschritt des Scanvorgangs und mögliche Fehler aufzeichnet. Ebenso wird die Scanausgabe in diesem Verzeichnis im CSV-Format gespeichert. Es kann sinnvoll sein, für jeden Scan ein anderes Repository-Verzeichnis zu verwenden. Dazu können Sie dem Befehl die Option -dir geben. Sehen Sie sich das folgende Beispiel an:

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

Mit dem obigen Befehl wird das TURKSAT-Netzwerk mit der ASN-Nummer (autonomes Netzwerk) 47524 durchsucht und die Entdeckungen im turksat-Verzeichnis gespeichert.

Verweise

Amass-Projekt-Website: https://owasp-amass.com/
Amass-Quellcode: https://github.com/OWASP/Amass
Benutzerhandbuch: https://github.com/OWASP/Amass/blob/master/doc / user_guide.md
Anwendungsbeispiele
: https://github.com/OWASP/Amass/blob/master/doc/tutorial.md
Benutzerhandbuch von Haklukes: https://hakluke.medium.com/haklukes-guide-to-amass- wie-man-masse-effektiver-für-bug-bounties-nutzt-7c37570b83f7

Urheberrechte ©

Das Kopieren im Rahmen des Teilens ohne Angabe der Quelle ist untersagt.