OWASPはユーザーマニュアルを蓄積します

著者：ÖzgürKoca、ozgurkoca.com、2022年6月

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

OWASP　Amassは、オープンソースの情報収集とアクティブな検出手法を使用して、攻撃ターゲットのネットワークマッピングと外部資産の検出を実行します。ここで、ツールがサブドメインを見つけるために使用する手法を確認してください。OWASPプロジェクトであるAmassは、オープンソースインテリジェンス（OSINT）の分野で使用される重要なブルーチームツールの1つです。Go言語で書かれたこのツールの主な焦点は、ドメイン名のインテリジェンスと発見です。

OWASP Amassツールは、データソースをスクレイピングし、ブルートフォースを再帰的に実行し、Webアーカイブをスキャンし、名前を許可/変更し、DNSスキャンを逆引きすることによってサブドメインを取得します。さらに、Amassは、解決中に取得したIPアドレスを使用して、関連するネットワークブロックとASNを検出します。次に、すべての情報を使用して、ターゲットネットワークのマップを作成します。アマスが使用する調査および発見技術には、次のものがあります。

- **変更/順列**：見つかったサブドメイン（dev1 <-> dev2）への基本的な変更。customer1.domain.comのようなサブドメインを見つけると、customer2.domain.comのような順次サブドメインもスキャンします。
- **ファジータグ/文字列検索**：加算減算（dev <-> dav）。dev.domain.comなどのサブドメインを見つけると、単純な文字の変更で可能なサブドメインを見つけようとします。
- **再帰的なブルートフォース**：APIとWEBアーカイブの検索。 wayback.comやarchiveit.comなどのアーカイブからサブドメインを検索します。彼が調査したデータソースは以下のとおりです。これらの一部は、APIキーを必要とする限定されたサービスです。
- **アクティブな手法**：HTTP　TLS/SSL証明書のダウンロード。共通名にはサブドメイン情報が含まれています。
- **ゾーン**：ゾーン転送とゾーンウォーキングの監視（NSECレコード）。
- **公開ソース**：Webアーカイブ、ペーストビン、バージョン管理、ソーシャルメディアのWebサイト。
- **証明書の透明性（CT）ログ**：CTは、証明書を追跡し、証明書が安全か悪意があるかを確認するために使用されるフレームワークです。ドメインに定義された証明書を使用して検出を試みます。
- **HTTP　CSP（コンテンツセキュリティポリシー）ヘッダー**：サブドメインがポリシーに含まれている場合、CSS攻撃からサブドメインを保護するために、ここでサブドメインがホワイトリストに登録されます。これにより、ホワイトリストに蓄積するためのデータソースが作成されます。

以下は、Amassが研究と発見に使用するデータソースです。次のコマンドを実行して、現在のデータソースとamassの可用性を確認できます。

```
amass enum -list
```

Amassは約50のデータソースを使用できます。そのうちのいくつかは無料で、いくつかは試用版で、いくつかは非常に高価なサービスです。コマンドに-srcパラメーターを追加して、最も成功したデータソースを追跡できます。したがって、どのソースが結果を返すか、およびその頻度を追跡できます。

テクニカル	情報源
API	360PassiveDNS、Ahrefs、AnubisDB、BinaryEdge、BufferOver、BuiltWith、C99、Chaos、CIRCL、Cloudflare、DNSDB、DNSRepo、Detectify、FOFA、FullHunt、GitHub、GitLab、Greynoise、HackerTarget、Hunter、IntelX、LeakIX、Maltiverse、MHT4

	5 PassiveTotal、Pentest 、Quake、Shodan、SonarSearch、Spamhaus、Spyse、Sublist3rAPI、ThreatBook、ThreatCrowd、ThreatMiner、Twitter、URLScan、VirusTotal、ZETAlytics、ZoomEye
証明書	アクティブプル（オプション）、Censys、CertSpotter、Crtsh、Digitorus、FacebookCT、GoogleCT
DNS	ブルートフォーシング、逆引きDNSスイープ、NSECゾーンウォーキング、ゾーン転送、FQDNの変更/順列、FQDNの類似性に基づく推測
オリエンテーション	ARIN、BGPTools、BGPView、IPdata、IPinfo、NetworksDB、RADb、Robtex、ShadowServer、TeamCymru
スクレイピング	AbuseIPDB、Ask、Baidu、Bing、DNSDumpster、DuckDuckGo、Gists、HackerOne、HyperStat、IPv4Info、PKey、RapidDNS、Riddler、Searchcode、Searx、SiteDossier、Yahoo
WEBアーカイブ	AlienVault、AskDNS、DNSlytics、ONYPHE、SecurityTrails、SpyOnWeb、Umbrella、WhoisXMLAPI
WHOISレコード	AlienVault、AskDNS、DNSlytics、ONYPHE、SecurityTrails、SpyOnWeb、Umbrella、WhoisXMLAPI

Amassは、非常に包括的で高度なツールです。このツールには、intel、enum、viz、track、dbの5つのサブコマンドが含まれています。 **Intel**コマンドは、ターゲットを偵察します。目的地の出発点を設定するのに便利です。 **enum**はターゲットをマップして、考えられる攻撃ポイントを特定します。 **viz**は、得られた結果を視覚化することにより、より良い分析に役立ちます。 **track**は、ターゲットの経時的な変化を追跡および比較するために使用されます。 amassは、すべてのインテリジェンスとスキャン結果を独自のデータベースに保存します。 **db**サブコマンドは、このデータベースにアクセスしてクエリを実行するために使用されます。ドキュメントページを参照して、amassのすべてのコマンドとオプションにアクセスできます。この章では、その基本的な使用法のみを例示します。

Amassサブコマンド

- **amass intel** ：ルートドメイン（サブドメインではない）、ASNを検出し、WHOISとDNSの逆引きクエリを実行します。対象組織の調査のためにオープンソースインテリジェンスを実施します。
- **amass enum** ：サブドメイン、高速モード（パッシブ）、通常モード、DNS解決/検証技術を使用して、オープンシステムのDNSレコードを抽出してマッピングします。
- **amass viz** ：視覚的な検査に適した視覚的なグラフィックを作成します。Maltegoをサポートします。行われた発見と研究の視覚的な図を作成します。
- **amass track** ：スキャンと新規または更新されたアセットの表示との間の履歴比較を可能にします。
- **amass db** ：Amassは、すべてのアクティブおよびパッシブ検出を独自のデータベースに保存します。dbコマンドは、後でこれらのレコードにアクセスするために使用されます。

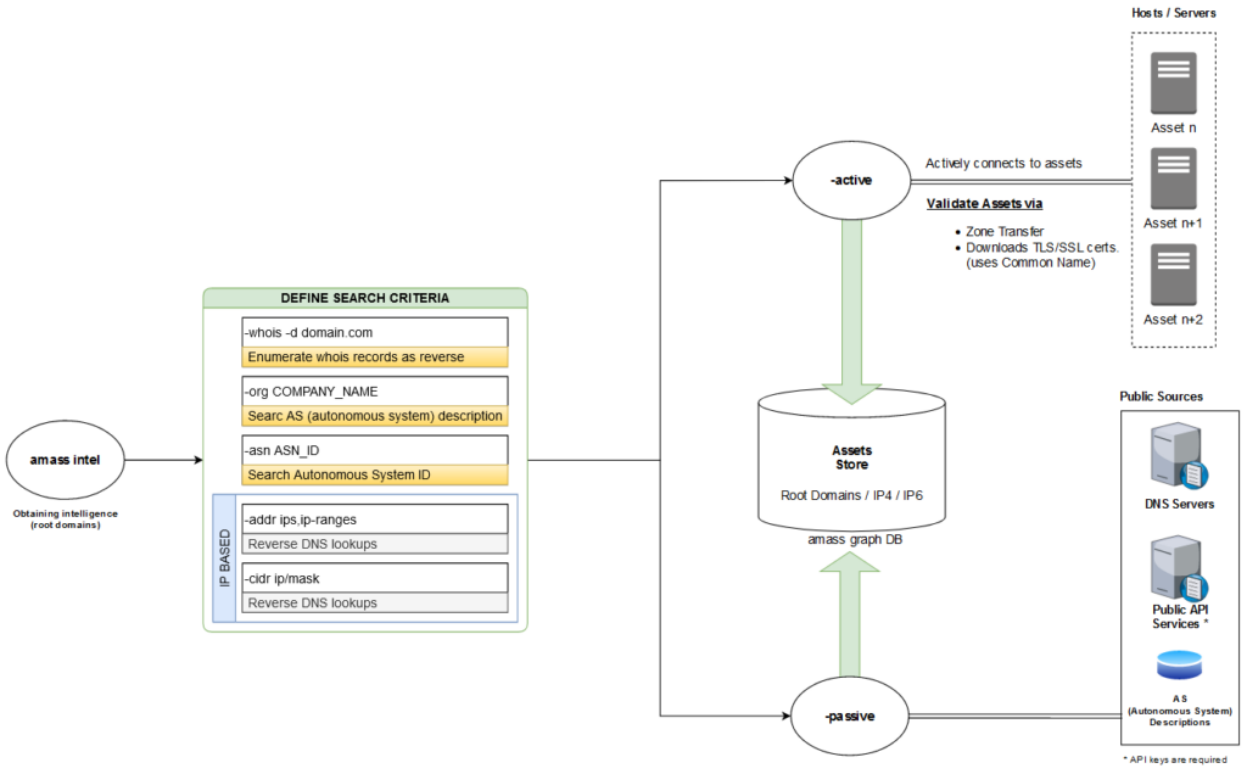
インテルコマンド

Amass　intelサブコマンド/モジュールは、企業に関するオープンソースインテリジェンスを収集するのに役立ち、企業に関連付けられているより多くのルートドメイン名を見つけることができます。このサブコマンドで使用可能なオプションを確認するには、ターミナルに次のように入力します。

```
$ amass intel
[...]
使用法：amassintel[オプション][-whois-d DOMAIN] [-addr ADDR -asn ASN -cidr CIDR]
-アクティブ
証明書名の取得を試みます
-addr値
カンマで区切られたIPと範囲（192.168.1.1-254）
-asn値
コンマで区切られたASN（複数回使用可能）
-cidr値
コンマで区切られたCIDR（複数回使用可能）
-org文字列
AS記述情報に対して提供される検索文字列
-誰が
提供されるすべてのドメインは、リバースwhoisを介して実行されます
```

[...]

この時点で、Amassのもう1つの大きな利点は、すべてのサブコマンドが引数の一貫性を維持しようとすることです。次の段落には、サブコマンドのパラメーターが含まれています。それらのほとんどが共通して使用されていることがわかります。次の図は、基本的に、アマスインテルの動作ロジックを示しています。



デフォルトでは、このサブコマンドは、Amassの構成ファイルで明示的に無効にされていない限り、一連の情報収集手法とWHOISやIPv4Infoなどのデータソースを使用して、組織のインテリジェンスと親ドメインを取得します。サンプルのAmass構成ファイルは、[GitHubリポジトリにあります。]

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

[...]

データソースを手動で参照することにより、上記の結果の一部を確認することもできます。以下のスクリーンショットでは、「OWASP Foundation」のWhois逆ルックアップを実行し、ViewDNS（これもAmassのデータソースの一部）に同様のドメインを要求しました。

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で検索する場合は、いつでもより多くの構成オプションを使用して実行できます。たとえば、-active引数を使用してゾーン転送を試行し、関連するサーバーに接続してSSL/TLS証明書を取得して情報を抽出できます。そうする前に、ターゲットに対してアクティブな検索を行う権限があることを確認してください。

この時点で、一部の構成フラグが他の構成フラグと連携しないことに注意してください。その場合、Amassはそれらを無視します。

Amassの調査結果は、さまざまな理由で常に正確であるとは限りません。たとえば、Amassが使用するデータソースは、一貫性がないか、最新ではない場合があります。 Amassは、DNSクエリを使用して情報をさらに検証しようとします。 Amassは優れた機能を果たしますが、ユーザーは、ターゲットに関連していないと思われる結果に対して、さらに多くの検証チェックを実行する必要があります。これは、次のようなさまざまな方法を使用して実行できます。

- ドメインを解決するには、ユーティリティ（dig、nslookupなど）を使用します。

- WHOIS検索を実行して、機関の詳細を確認します。
- 検索エンジンのメインドメインのような検索結果を使用します。

amassintel-orgトルコ

トルコという単語に関連するASNIDを返します。このタイプの文字列検索では、多くの場合、十分な結果が返されません。アクティブなメソッドを使用して検索を実行する場合は、-activeスイッチを追加することもできます。上記のコマンドは、ASNの説明でトルコを検索し、関連するASNを返します。

orgキーは、指定された式に関連付けられたASN ID（自律システム）を検索します。-orgパラメーターで指定された文字列がASレコードで検索され、そのASNIDが検出されます。 ASN IDは、Internet Assigned Numbers Authority（IANA）によって割り当てられた自律システム番号であり、世界的に一意の16桁の識別番号で表されます。 AS（自律システム）とは、単一のルーティングポリシー（rfc1930）を持つ大規模なネットワークまたはネットワークのグループを指します。 ASNIDでそれらを識別します。たとえば、TTNETのネットワークのASN番号は9121、CloudFlareの13335、ULAKNETの8517、Amazonの16509です。大規模なルーターは、ネットワーク間でルーティングを行う必要がある場合に、これらのASN番号を利用します。

次に、見つかったASNでドメイン名を見つけてみましょう。以下のコマンドを確認してください。

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

ASN番号8517の自律ネットワーク（ULAKNET）のドメインのポート80および443でアクティブな手法（-active）を使用して検出を行います。アクティブな検出にはTLS/SSL証明書を使用します。 amassは、指定されたASNのすべてのIPアドレスに接続するSSL証明書をプルし、SSL証明書が関連付けられているドメインを一覧表示します。また、検出したドメインの送信元（-src）アドレスとip（-ip）アドレスも表示されます。

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

文字列範囲は、-cidrパラメーターで宣言されます。数字の24はネットマスクを表し、255.255.255.0に対応します。 amassは、193.140.28.1から193.140.28.254までのIPアドレスのさまざまなソースを検索して検出し、これらのIPに向けられたドメイン名を検出して一覧表示します。また、アクティブな検出は、ポート80および443のTLS/SSL証明書を使用して実行されます。各IPアドレスに接続し、SSL証明書をプルして、証明書に記載されているドメイン名を一覧表示します。

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

アクティブな技術を使用して、ネットワーク74.6.0.6/16のコンピューターをスキャンします。見つかったドメインのIPアドレスとソースが一覧表示されます。74.6.231.20-21の範囲のコンピューターで逆引きDNSクエリを実行します。

amass intel -whois -d yahoo.com

指定されたドメイン（-d）またはドメインリスト（-df）のWHOISレコードを逆検索して、ドメイン名を検索しようとします。この例では、amassはyahoo.comのWHOISレコードにアクセスし、それらのWHOISレコードと同じである可能性のある他の組織のルートドメインを見つけようとします。組織/会社に属する他のドメインを見つけるのに役立ちますが、WHOISレコードには常に正確な情報が含まれているとは限らず、機密が保持されているとは限りません。

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

このコマンドは、ASNID8517のULAKNET自律ネットワークで同じWHOISレコードを持つ他のドメインを検索します。

以下は、intelコマンドのオプションと使用領域を示す表です。

選択	説明	サンプル
-アクティブ	アクティブなメソッドを使用します。ゾーンは転送を試み、ターゲットサーバーに接続してSSL/TLS証明書を取得します。	amass intel -active -addr 192.168.2.1-64 -p 80,443,8080
-ADDR	IP範囲を指定します。範囲はコンマで区切られます。	192.168.2.1-64,192.168.3.10-254

-ASN	ASNIDを報告します。 ASN IDは、IANNAによって大規模なコンピューターネットワークに割り当てられた一意の番号です。	amass intel -asn 13374,14618
-CIDR	ネットワークを定義します。スラッシュの後の数字はネットマスクを定義します。	amass intel -cidr 104.154.0.0/15
-CONFIG	スキャン構成ファイルの場所を指定します。	amass intel -config config.ini
-D	カンマで区切られたフィールド名。	amass intel -whois -d example.com
-DF	ファイルからルートドメインをフィードします。	amass intel -whois -df domains.txt
は	スキャン結果が保存されるデータベースを含むディレクトリへのパスを指定します。	amass intel -dir PATH -cidr 104.154.0.0/15
-EF	調査時に使用されないデータソースのリストを含むファイルへのパス。	amass intel -whois -ef Exclusive.txt -d example.com
-除外	スキャンに使用されないデータソースのリスト。カンマで区切って指定します。	amass intel -whois -exclude crtsh -d example.com
-もしも	スキャンに使用するデータソースのリストを含むファイルへのパス。	amass intel -whois -if include.txt -d example.com
-含む	スキャンに使用するデータソースのリスト。カンマで区切って記述します。	amass intel -whois -include crtsh -d example.com
-ループ	また、検出されたドメインのIPアドレスも表示されます。	amass intel -ip -whois -d example.com
-IPV4	また、検出されたドメインのIPv4アドレスも表示されます。	amass intel -ipv4 -whois -d example.com
-IPV6	また、検出されたドメインのIPv6アドレスも表示されます。	amass intel -ipv6 -whois -d example.com
-リスト	検出に使用するデータソースを一覧表示します。	amass intel -list
-ログ	エラーがログに記録されるログファイルへのパスを報告します。	amass intel -log amass.log -whois -d example.com

-MAX-DNS-クエリ	同時DNSクエリの最大数。	amass intel -max-dns-queries 200 -whois -d example.com
-彼	出力が保存されるファイルへのパス。	amass intel -o out.txt -whois -d example.com
-器官	ASステートメントで検索する文字列式。	amass intel -org Facebook
-P	カンマ区切りのポート番号。	amass intel -cidr 104.154.0.0/15 -p 443,8080
-R	検出中に使用されるDNSサーバーを宣言します。	amass intel -r 8.8.8.8,1.1.1.1 -whois -d example.com
-RF	検出中に使用されるDNSサーバーのリストを含むファイルのパスを示します。	amass intel -rf data / resolvers.txt -whois -d example.com
-SRC	検出されたフィールドが取得されたソースを示します。	amass intel -src -whois -d example.com
-タイムアウト	検出中に考慮するタイムアウト期間。	amass intel -timeout 30 -d example.com
-誰が	WHOIS情報は、他の同様のドメインを検索します。	amass intel -whois -d example.com

amassenumコマンド

Amass列挙型は、パッシブモードまたはアクティブモードで実行できます。パッシブモードははるかに高速ですが、Amassはサブドメインを解決することによってDNS情報を検証しません。 「-passive」フラグを使用してパッシブに実行でき、DNS解決や検証などの多くの手法や構成を有効にすることはできません。たとえば、アクティブモードではなくパッシブモードを選択する必要がある場合があります。

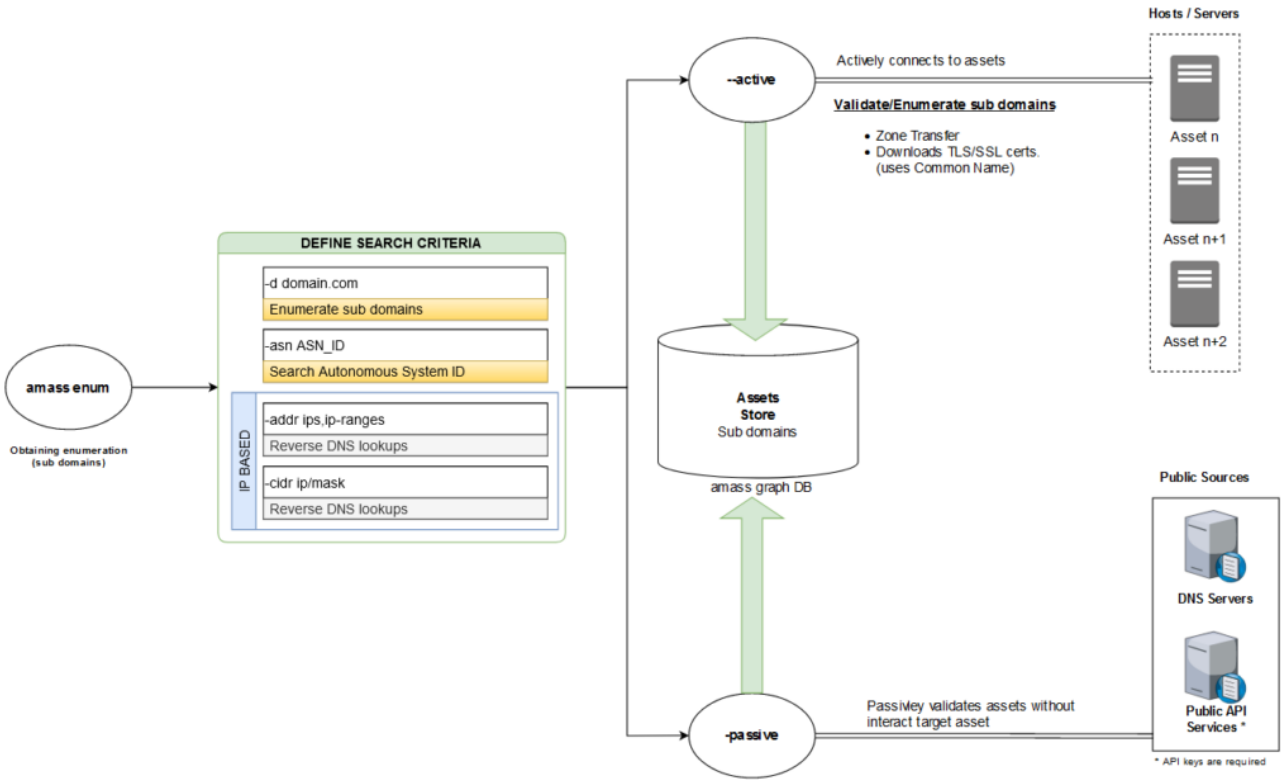
- ターゲットスコープの変更を常に監視する必要があるため、またはフィッシングインタラクションに取り組んでいてサブドメインを検索しているため、使用されており、将来再利用される可能性のあるすべてのサブドメインを知る必要があります。
- 後の段階でDNS情報を確認し、結果をすばやくスプールする必要がある場合があります。

- セキュリティエンゲージメントの制約または要件により、受動的な情報収集のみを実行する必要がある場合があります。

このサブコマンドで使用可能なオプションを確認するには、ターミナルに次のように入力します。

使用法：列挙型を蓄積[オプション] -d DOMAIN

-アクティブ
ゾーン転送と証明書名の取得を試行します
-addr値
カンマで区切られたIPと範囲（192.168.1.1-254）
-d値
カンマで区切られたドメイン名（複数回使用可能）
-cidr値
コンマで区切られたCIDR（複数回使用可能）
-asn値
コンマで区切られたASN（複数回使用可能）



以下の例では、Owasp.orgでサブドメインを受動的に検索し、各サブドメインが見つかったデータソースを表示するようにAmassに要求しています。

```
$ 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
[...]
owasp.orgサブドメインのVirusTotalのクエリ
Yahooasp.orgサブドメインのクエリ
[...]
```

このサブコマンドは、プローブ中にDNS検出とネットワークマッピングを実行します。この時点で、 Amass 列挙型がすべてのサブドメインを識別することに注意してください。ただし、 Amass intelコマンドは、組織が所有するIP範囲、ASN、およびメインドメインを収集するのに役立ちます。

アクティブ構成モードでAmassを使用すると、すべてのDNS検出手法を有効にできるため、より正確な結果が得られ、より多くのアセットを検出できるようになります。「有効な構成モード」では、 SSL / TLS サービスのゾーン転送とポートスキャンを実行することにより、証明書ドメイン（例：共通名）からサブドメインを検索します。

は、「-active」フラグを有効にして複数の方法（単語リスト、マスクなど）でサブドメインブルートフォーシングを実行するため、一般にアクティブと見なすことができます。すべての調査結果は、デフォルトまたは指定されたアナライザーを使用してAmassによって検証されます。

以下のすべての設定は、このサブコマンドに関連しています。次のフラグを構成に使用できます。

選択	***説明***	***サンプル***
-アクティブ	アクティブなメソッドを使用します。ゾーンは転送を試み、ターゲットサーバーに接続してSSL/TLS証明書を取得します。	amass enum -active -d example.com -p 80,443,8080
-aw	サブドメインの代替を生成するための代替単語ファイルのパスを示します。	amass enum -aw PATH -d example.com
-bl	検出されないサブドメインのブラックリストを報告します。	amass enum -bl blah.example.com -d example.com

-blf	ブラックリストに登録されたサブドメインのリストとともにファイルのパスを指定します。	amass enum -blf data / blacklist.txt -d example.com
-野蛮人	サブドメイン探索でブルートフォースを使用します。	amass enum -brute -d example.com
-config	INI構成ファイルへのパスを指定します。	amass enum -config config.ini
-D	カンマで区切られたフィールド名。	amass enum -d example.com
-df	ファイルからルートドメインをフィードします。	amass enum -df domains.txt
は	スキャン結果が保存されるデータベースを含むディレクトリへのパスを指定します。	amass enum -dir PATH -d example.com
-ef	調査時に使用されないデータソースのリストを含むファイルへのパス。	amass enum -ef extract.txt -d example.com
-除外する	スキャンに使用されないデータソースのリスト。カンマで区切って指定します。	amass enum -ef extract.txt -d example.com
-もしも	スキャンに使用するデータソースのリストを含むファイルへのパス。	amass enum -ef extract.txt -d example.com
-含む	スキャンに使用するデータソースのリスト。カンマで区切って記述します。	amass enum -include crtsh -d example.com
-ループ	また、検出されたドメインのIPアドレスも表示されます。	amass enum -ip -d example.com
-ipv4	また、検出されたドメインのIPv4アドレスも表示されます。	amass enum -ip -d example.com
-ipv6	また、検出されたドメインのIPv6アドレスも表示されます。	amass enum -ip -d example.com
-json	JSON形式で保存する出力ファイルのパスを定義します。	amass enum -json out.json -d example.com
-リスト	検出に使用するデータソースを一覧表示します。	amass enum -list
-ログ	エラーがログに記録されるログファイルへのパスを報告します。	amass enum -log amass.log -d example.com

-max-dns-クエリ	同時DNSクエリの最大数。	amass enum -max-dns-queries 200 -d example.com
-dns-qps	すべてのドメインリゾルバー（DNSサーバー）での1秒あたりのDNSクエリの最大数。	amass enum -dns-qps 200 -d example.com
-rqps	信頼できないリゾルバーごとの1秒あたりのDNSクエリの最大数。	amass enum -dns-qps 200 -d example.com
-trqps	信頼できるリゾルバーごとの1秒あたりのDNSクエリの最大数	amass enum -trqps 20 -d example.com
-min-for-recursive	再帰的なブルートフォーシングの前に表示されるサブドメインラベル（デフォルト：1）	amass enum -brute -min-for-recursive 3 -d example.com
-最大深度	ブルートフォーシングのサブドメインタグの最大数	amass enum -brute -max-depth 3 -d example.com
-nf	（他のツール/ソースからの）既知のサブドメインを提供するファイルへのパス	amass enum -nf names.txt -d example.com
-noalts	代替サブドメインの生成を無効にします。	amass enum -noalts -d example.com
-再帰的ではありません	再帰的なブルートフォースを無効にします。	amass enum -brute -norecursive -d example.com
-彼	テキスト出力ファイルへのパスを指定します。	amass enum -o out.txt -d example.com
-oA	すべての出力ファイルに名前を付けるために使用されるパスプレフィックス。	amass enum -oA amass_scan -d example.com
-受け身	完全にパッシブな実行を実行します。	amass enum --passive -d example.com
-p	カンマ区切りのポート番号。	amass enum -d example.com -p 443,8080
-r	検出中に使用されるDNSサーバーを宣言します。	amass enum -d example.com -p 443,8080
-en	信頼できるDNSリゾルバーのIPアドレス（複数回使用可能）	amass enum -en 8.8.8.8,1.1.1.1 -d example.com

-rf	検出中に使用されるDNSサーバーのリストを含むファイルのパスを示します。	amass enum -en 8.8.8.8,1.1.1.1 -d example.com
-trf	信頼できるDNSリゾルバーを提供するファイルへのパスを指定します。	amass enum -trf data / trusted.txt -d example.com
-src	検出されたフィールドが取得されたソースを示します。	amass enum -src -d example.com
-タイムアウト	検出中に考慮するタイムアウト期間。	amass enum -timeout 30 -d example.com
-w	別のワードリストファイルのパスを報告します。	amass enum -brute -w wordlist.txt -d example.com

enumコマンドの最も一般的な使用法は次のとおりです。このコマンドが与えられた後、amassはインターネットからmeb.gov.trドメイン名のサブドメインの検索を開始します。可能なすべてのデータソースに問い合わせ、サブドメインのスタックを返します。

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

このスキャンでは、（パッシブ）スキャンがDNS解決なしで実行されます。 Passive-config.iniにパッシブ情報リソースとAPIキーのリストが含まれていると仮定します。 -passiveオプションは、-activeよりも高速ですが、結果は少なくなります。

-vパラメーターを使用すると、amass.logファイルの詳細レベルを上げて、適用中にamassの機能をよりよく理解できます。これにより、正しく機能していないデータソースを検出したり、IPアドレスをブロックしているサービスを確認したり、正しく機能していないDNSリゾルバーを確認したりできます。

amasstrackコマンド

ターゲットの攻撃対象領域を監視するために、同じターゲットの偵察の違いを示します。このサブコマンドは、「output_directory」と構成ファイルで指定されたリモートデータベース設定のみを利用します。

このサブコマンドで使用可能なオプションを確認するには、ターミナルに次のように入力します。

使用法：アマストラック[オプション]-dドメイン

-d値
カンマで区切られたドメイン名（複数回使用可能）
-歴史
すべての列挙ペアの違いを表示する
-最後のint
追跡に含める最近の列挙の数

選択	*説明*	*サンプル*
-config	INI構成ファイルへのパスを指定します。	amass track -config config.ini
-D	カンマで区切られたフィールド名。	アマストラック-dexample.com
-df	ファイルからルートドメインをフィードします。	アマストラック-dfdomains.txt
は	スキャン結果が保存されるデータベースを含むディレクトリへのパスを指定します。	アマストラック-dfdomains.txt
-歴史	発見の違いを示しています。	アマストラック-歴史
-過去	追跡に含める最近の発見の数。	アマストラック-最後の2
-以来	指定された日付より前のすべての列挙を除外します（形式：01/02 15:04:05 2006 MST）	アマストラック-DATE以降

amass track -d yahoo.com -last 2

上記のコマンドは、ドメインyahoo.comの最後の2つのスキャンを比較します。

amassvizコマンド

収集した情報を使用して、視覚的なネットワークグラフを作成します。この視覚化は、包括的な結果を返す大規模なスキャンでエンティティ間の関係を解釈する場合に特に役立ちます。このサブコマンドは、構成ファイルの「output_directory」およびリモートグラフィックデータベース設定のみを利用します。

視覚化のために作成されたファイルは、デフォルトで現在の作業ディレクトリに作成されます。 DNSとインフラストラクチャの結果をネットワークグラフとして出力するために使用できるスイッチは次のとおりです。

選択	*説明*	*サンプル*
-config	INI構成ファイルへのパスを指定します。	amass viz -config config.ini -d3
-D	カンマで区切られたフィールド名。	amass viz -d3 -d example.com
-d3	D3.jsv4形式のHTMLシミュレーションファイルを生成します。	amass viz -d3 -d example.com
-df	ルートドメインを含むファイルへのパスを定義します。	amass viz -d3 -df domains.txt
は	グラフデータベースを含むディレクトリへのパスを定義します。	amass viz -d3 -dir PATH -d example.com
-列挙型	スキャン結果は、データベースからのインデックス番号によって検出を識別します。	amass viz -enum 1 -d3 -d example.com
-彼	出力ファイルが保存されるディレクトリへのパスを定義します。	amass viz -d3 -o OUTPATH -d example.com
-oA	出力ファイルのプレフィックスを定義します。	amass viz -d3 -oA example -d example.com
-gexf	グラフ交換XML形式（GEXF）形式で出力します。	amass viz -gexf -d example.com
-グラフィストリー	GraphistryはJSON形式の出力を返します。	amass viz -graphistry -d example.com
-maltego	Maltegoグラフテーブル形式のCSVファイルを出力します。	amass viz -maltego -d example.com

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

上記のコマンドは、ドメインyahoo.comのすべての結果を、連想グラフ付きのHTML形式のファイルで表示します。チャートは、d3javascriptライブラリを使用して作成されます。-oオプションを使用すると、出力はyahooディレクトリに保存されます。　vizzコマンドは、Maltego、XML、およびJSON形式で出力することもできます。

amassdbコマンド

これは、実行された各スキャンの検出データを表示できるようにするコマンドです。データベースの表示と処理を実行します。このサブコマンドは、構成ファイルの「output_directory」およびリモートデータベース設定のみを利用します。データベース内の探索結果を操作するための使用オプションは次のとおりです。

選択	説明	サンプル
-CONFIG	INI構成ファイルへのパスを指定します。	amass db -config config.ini
-D	カンマで区切られたフィールド名。	amass db -d example.com
-DF	ファイルからルートドメインをフィードします。	amass db -df domains.txt
は	スキャン結果を含むデータベースディレクトリへのパスを指定します。	amass db -dir PATH
-列挙型	リストからインデックスシーケンス番号を介して検出情報を取得します。	amass db -enum 1 -show
-輸入	JSON形式のamassファイルをインポートします。	amass db -import PATH
-ロープ	また、検出されたドメインのIPアドレスも表示されます。	amass db -show -ip -d example.com
-IPV4	また、検出されたドメインのIPv4アドレスも表示されます。	amass db -show -ipv4 -d example.com
-IPV6	また、検出されたドメインのIPv6アドレスも表示されます。	amass db -show -ipv6 -d example.com
-JSON	JSON形式で保存する出力ファイルのパスを定義します。	amass db -names -silent -json out.json -d example.com
-リスト	検出に使用するデータソースを一覧表示します。	amass db -list
-名前	検出されたドメインのみを取得します。	amass db -names -d example.com
-NOCOLOR	カラー出力を無効にします。	amass db -names -nocolor -d example.com

-彼	テキスト出力ファイルへのパスを指定します。	amass db -names -o out.txt -d example.com
-見せる	結果の検出ディレクトリ+ドメインの結果を出力します。	amass db -show
-静けさ	実行中のすべての出力を無効にします。	amass db -names -silent -json out.json -d example.com
-SRC	検出されたフィールドが取得されたソースを示します。	amass db -show -src -d example.com
-まとめ	ASNテーブルの要約のみを出力します。	amass db -summary -d example.com

以前のスキャンのすべての詳細を一覧表示するには、amass db -showを実行するだけで、新しいスキャンを行わなくても現在の結果を確認できます。特定のドメインの詳細を表示したい場合は、-dオプションを追加するだけです。

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

きれいでシンプルな出力が必要な場合は、-showの代わりに-namesオプションを使用して、検出されたドメイン/サブドメインを印刷できます。

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

amass4owaspディレクトリに登録されているデータベースのドメイン名owasp.orgの検出＃1の結果を表示します。

APIキーの生成

Amassが使用できるデータソースはたくさんあります。記事の冒頭でそれらのリストを示しました。ただし、以下にリストされているデータソースにはAPIキーが必要です。

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

これらのAPIキーのほとんどは無料ですが、有料のAPIキーを持っていない限り、ほとんどの場合、限られた結果しか得られません。無料のものは何もないよりはましです。上記の各サービスのWebサイトを見つけてから、サインアップしてAPIキーを取得する必要があります。これは非常に時間のかかる退屈な作業ですが、犠牲を払わずに良い発見をすることはできません。あなたはこれを行うことができます。すべてのAPIキーを取得したら、それらをamass構成ファイルに貼り付けます。包括的な設定ファイルの例については、こちらをご覧ください。以下は、構成ファイルの内容です。有料を書いた人は有料です。サンプルファイルのAPIを使用してデータソースを取得し、次のように追加して、独自のamass構成ファイルを作成します。次に、ファイルをamassconfig.iniという名前で保存します。例：

```
＃https：//passivedns.cn（連絡先）
[data_sources.360PassiveDNS]
[ data_sources.360PassiveDNS.Credentials ]
apikey = sizeozelapicode

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

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

ここで、amassを使用する場合は、次のように-configパラメーターを指定して構成ファイルを指定します。これにより、Intelと列挙型の発見の数と質が向上します。他の一歩先を行くために、これを行うことを強くお勧めします。

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

出力ディレクトリ

amassは、最後のスキャンセッションのログファイルと出力ファイルをデフォルトで～/ .config/amassに保持します。これらのファイルは、新しいスキャンが行われるとリセットされます。ログファイルは、スキャンプロセスの進行状況と発生する可能性のあるエラーを記録するため、スキャンの最後に調べる必要があります。同様に、スキャン出力はこのディレクトリにCSV形式で保存されます。スキャンごとに異なるリポジトリディレクトリを使用すると便利な場合があります。このためのコマンドに-dirオプションを指定できます。以下の例を確認してください。

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

上記のコマンドを使用すると、ASN（自律ネットワーク）番号47524のTURKSATネットワークが検索され、検出されたものがturksatディレクトリに保存されます。

参考文献

AmassプロジェクトのWebサイト： https ：
//owasp-amass.com/ Amassソースコード： https ：//github.com/OWASP/Amass
ユーザーガイド： https：//github.com/OWASP/Amass/blob/master/doc / user_guide.md
使用例： https ：//github.com/OWASP/Amass/blob/master/doc/tutorial.md
Haklukesのユーザーガイド： https：//hakluke.medium.com/haklukes-guide-to- amass- how-to-use-amass-more-effectively-for-bug-bounties-7c37570b83f7

著作権