OWASP 用户手册

作者：Özgür Koca，ozgurkoca.com，2022 年 6 月

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

OWASP Amass使用开源信息收集和主动发现技术执行攻击目标的网络映射和外部资产发现。在此处查看该工具用于查找子域的技术。 OWASP项目Amass是开源智能（OSINT）领域使用的重要蓝队工具之一。用Go语言编写，该工具的主要重点是域名智能和发现。

OWASP Amass 工具通过抓取数据源、递归暴力破解、扫描 Web 档案、允许/更改名称以及反向 DNS 扫描来获取子域。此外，Amass 使用在解析过程中获得的 IP 地址来发现相关的网络块和 ASN。然后使用所有信息来创建目标网络的地图。Amass 使用的研究和发现技术包括：

- **修改/排列**：对找到的子域（dev1 <-> dev2）的原始更改。当它看到诸如 customer1.domain.com 之类的子域时，它还会扫描诸如 customer2.domain.com 之类的顺序子域。

- **模糊标签/字符串搜索**：加减法（dev <-> dav）。当它看到诸如 dev.domain.com 之类的子域时，它会尝试通过简单的字母更改来查找可能的子域。
- **递归蛮力**：搜索 API 和 WEB 档案。它从诸如wayback.com 和archiveit.com 之类的档案中搜索子域。下面列出了他探索的数据源。其中一些是需要 API 密钥的有限服务。
- **主动技术**：下载 HTTP TLS/SSL 证书。Common Name 包含子域信息。
- **区域**：监控区域转移和区域行走（NSEC 记录）。
- **公共资源**：Web 档案、pastebin、版本控制和社交媒体网站。
- **Certificate Transparancey (CT) 日志**：CT 是用于跟踪证书并验证证书是安全还是恶意的框架。它尝试使用为域定义的证书进行发现。
- **HTTP CSP（内容安全策略）标头**：当策略中包含子域时，它们会在此处被列入白名单，以保护它们免受 CSS 攻击。这会为白名单中的 amass 创建一个数据源。

以下是 Amass 用于研究和发现的数据源。您可以运行以下命令来查看当前数据源和 amass 的可用性。

amass 枚举列表

Amass 可以使用大约 50 个数据源，其中一些是免费的，一些是试用版，一些是非常昂贵的服务。您可以将 -src 参数添加到命令中以跟踪最成功的数据源。因此，您可以跟踪哪个来源返回结果以及频率。

技术的	数据源
蜜蜂	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
证书	主动拉取（可选）、Censys、CertSpotter、Crtsh、Digitorus、FacebookCT、Google CT

域名系统	暴力破解、反向 DNS 扫描、NSEC 区域遍历、区域传输、FQDN 更改/排列、FQDN 基于相似性的猜测
方向	ARIN、BGPTools、BGPView、IPdata、IPinfo、NetworksDB、RADb、Robtex、ShadowServer、TeamCymru
刮	AbuseIPDB、Ask、百度、Bing、DNSDumpster、DuckDuckGo、Gists、HackerOne、HyperStat、IPv4Info、PKey、RapidDNS、Riddler、Searchcode、Searx、SiteDossier、Yahoo
网络档案	AlienVault、AskDNS、DNSlytics、ONYPHE、SecurityTrails、SpyOnWeb、Umbrella、WhoisXMLAPI
WHOIS 记录	AlienVault、AskDNS、DNSlytics、ONYPHE、SecurityTrails、SpyOnWeb、Umbrella、WhoisXMLAPI

Amass 是一个非常全面和先进的工具。该工具包含 5 个子命令， intel、enum、viz、track 和 db。 **intel**命令对目标进行侦察。用于设置目的地的起点。 **enum**映射目标以识别可能的攻击点。**即**通过可视化获得的结果有助于更好地分析。 **track**用于跟踪和比较目标随时间的变化。amass 将所有情报和扫描结果保存在自己的数据库中。**db**子命令用于访问和查询该数据库。您可以参考文档页面来访问 amass 的所有命令和选项。在本章中， 我将仅举例说明它的基本用途。

积累子命令

- **amass intel** ：发现根域（不是子域）、ASN、执行反向 WHOIS 和 DNS 查询。它为目标组织的调查进行开源情报。
- **amass enum** ：使用子域、快速模式（被动）、正常模式、DNS 解析/验证技术提取和映射开放系统的 DNS 记录。
- **amass viz** ：创建视觉图形， 有利于视觉检查。支持马尔特戈。创建发现和研究的可视化图表。

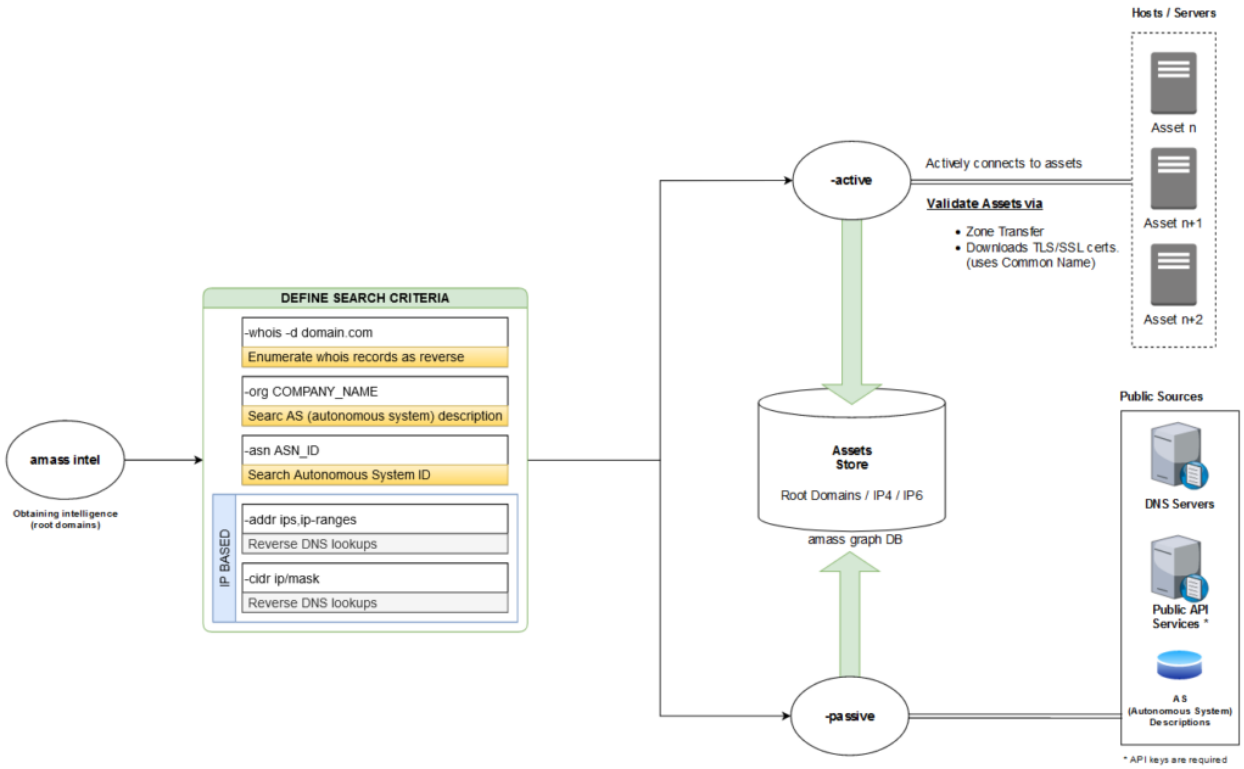
- **amass track** ：允许在扫描和查看新资产或更新资产之间进行历史比较。
- **amass db** ：Amass 将所有主动和被动发现存储在自己的数据库中。db 命令用于稍后访问这些记录。

英特尔命令

Amass intel 子命令/模块可以帮助收集有关企业的开源情报，并允许您找到与企业相关的更多根域名。要查看此子命令的可用选项，只需在终端中输入：

```
$积累英特尔
[...]
用法：amass intel [options] [-whois -d DOMAIN] [-addr ADDR -asn ASN -cidr CIDR]
-积极的
尝试证书名称抓取
-addr 值
IP 和范围 (192.168.1.1-254) 以逗号分隔
-asn 值
以逗号分隔的 ASN（可多次使用）
-cidr 值
以逗号分隔的 CIDR（可多次使用）
-org 字符串
针对 AS 描述信息提供的搜索字符串
-谁是
所有提供的域都通过反向 whois 运行
[...]
```

在这一点上，值得注意的是，Amass 的另一大优势是所有子命令都试图保持参数的一致性。在下面的段落中，包含了子命令的参数，您可以看到它们中的大多数是通用的。下图基本展示了amass intel的工作逻辑。



默认情况下，除非在 Amass 的配置文件中明确禁用，否则此子命令将使用一组信息收集技术和数据源（例如 WHOIS 和 IPv4Info）来获取组织情报和父域。GitHub 存储库中提供了一个示例 Amass 配置文件。

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

您还可以通过手动浏览数据源来确认上述部分结果。在下面的屏幕截图中，我们对“OWASP Foundation”进行了反向 Whois 查找，并向 ViewDNS（也是 Amass 数据源的一部分）询问了类似域：

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

使用 Amass intel 搜索时，您始终可以使用更多配置选项运行它，例如，您可以尝试使用 --active 参数进行区域传输，并让它连接到相关服务器以获取 SSL/TLS 证书以提取信息。只需确保您有权在执行此操作之前对目标进行主动搜索。

在这一点上，值得注意的是一些配置标志将无法与其他配置标志一起使用，在这种情况下，Amass 将忽略它们。

由于各种原因，Amass 的调查结果可能并不总是准确的，例如，Amass 使用的数据源可能不一致或不是最新的。Amass 尝试使用 DNS 查询进一步验证信息。虽然 Amass 做得很好，但用户仍然应该对似乎与目标无关的结果进行更多的验证检查。这可以使用多种方法来完成，例如：

- 使用实用程序（例如 dig、nslookup）来解析域。
- 执行 WHOIS 搜索以验证机构详细信息。
- 使用搜索结果，如搜索引擎中的主要域。

amass intel -org 土耳其

返回与单词土耳其相关的 ASN ID。这种类型的字符串搜索通常不会返回足够的结果。如果您还希望使用活动方法执行搜索，也可以添加 -active 开关。上述命令将在 ASN 描述中搜索土耳其并返回关联的 ASN。

org 关键字搜索与给定表达式关联的 ASN ID（自治系统）。在 AS 记录中搜索使用 -org 参数指定的字符串并找到其 ASN ID。ASN ID 是互联网号码分配机构 (IANA) 分配的自治系统编号，它由全球唯一的 16 位标识号表示。AS（自治系统）是指具有单一路由策略 (rfc1930) 的大型网络或网络组。在 ASN ID 中标识它们。例如TTNET的网络ASN号为9121，CloudFlare的为13335，ULAKNET的为8517，亚马逊的为16509。当需要在网络之间进行路由时，大型路由器会利用这些 ASN 编号。

现在让我们尝试在我们找到的 ASN 中查找域名。查看下面的命令。

积累英特尔-active -src -ip -asn 8517 -p 80,443

它将使用主动技术 (-active) 在 ASN 号为 8517 的自治网络 (ULAKNET) 中的域的端口 80 和 443 上进行发现。它将使用 TLS/SSL 证书进行主动发现。amass 将提取 SSL 证书，该证书将连接到指定 ASN 的所有 IP 地址，并列出与 SSL 证书关联的域。它还将显示它找到的域的源 (-src) 和 ip (-ip) 地址。

积累英特尔-active -ip -src -cidr 193.140.28.0/24 -p 80,443

使用 -cidr 参数声明字符串范围。数字 24 代表网络掩码，对应 255.255.255.0。amass 将搜索并发现 193.140.28.1 和 193.140.28.254 之间的 IP 地址的不同来源，检测并列出指向这些 IP 的域名。此外，将使用端口 80 和 443 的 TLS/SSL 证书进行主动发现。它将连接到每个 IP 地址并提取 SSL 证书并列出证书中提到的域名。

积累英特尔-active -ip -src -cidr 74.6.0.6/16 -addr 74.6.231.20-21 -p 80.8080

它将使用主动技术扫描网络 74.6.0.6/16 中的计算机。它将列出找到的域的 IP 地址和来源。它将在 74.6.231.20-21 范围内的计算机上执行反向 DNS 查询。

积累英特尔-whois -d yahoo.com

它尝试通过反向搜索给定域 (-d) 或域列表 (-df) 的 WHOIS 记录来查找域名。在此示例中，amass 访问 yahoo.com 的 WHOIS 记录并尝试查找可能与这些 WHOIS 记录相同的其他组织的根域。它对于查找属于组织/公司的其他域很有用，但 WHOIS 记录可能并不总是包含准确的信息或保密。

积累英特尔-asn 8517 -whois -d omu.edu.tr

此命令在 ASN ID 为 8517 的 ULAKNET 自治网络中搜索具有相同 WHOIS 记录的其他域。

下表显示了 intel 命令的选项和使用范围。

选择	解释	样本
-积极的	它使用主动方法。 Zone 尝试传输，连接到目标服务器以获取 SSL/TLS 证书。	积累英特尔-active -addr 192.168.2.1-64 -p 80,443,8080
-地址	指定 IP 范围。范围用逗号分隔。	192.168.2.1-64,192.168.3.10-254
-ASN	报告 ASN ID。ASN ID 是 IANNA 分配给大型计算机网络的唯一编号。	积累英特尔-asn 13374,14618
-CIDR	定义一个网络。斜杠后面的数字定义网络掩码。	积累英特尔-cidr 104.154.0.0/15
-配置	指定扫描配置文件的位置。	积累英特尔-config config.ini
-D	用逗号分隔的字段名称。	amass intel -whois -d example.com
-DF	它从文件中提供根域。	积累英特尔 -whois -df domain.txt
是	指定包含将存储扫描结果的数据库的目录的路径。	积累英特尔 -dir PATH -cidr 104.154.0.0/15
-EF	文件的路径，其中包含研究时不会使用的数据源列表。	amass intel -whois -ef exclude.txt -d example.com
-排除	不会在扫描中使用的数据源列表。它通过用逗号分隔来指定。	amass intel -whois -exclude crtsh -d example.com
-如果	包含用于扫描的数据源列表的文件的路径。	amass intel -whois -if include.txt -d example.com

-包括	用于扫描的数据源列表。它以逗号分隔。	amass intel -whois -include crtsh -d example.com
-绳索	它还显示已发现域的 IP 地址。	amass intel -ip -whois -d example.com
-IPV4	它还显示已发现域的 IPv4 地址。	amass intel -ipv4 -whois -d example.com
-IPV6	它还显示已发现域的 IPv6 地址。	amass intel -ipv6 -whois -d example.com
-列表	列出要在发现中使用的数据源。	积累英特尔列表
-日志	报告将记录错误的日志文件的路径。	amass intel -log amass.log -whois -d example.com
-MAX-DNS-查询	最大并发 DNS 查询数。	amass intel -max-dns-queries 200 -whois -d example.com
-他	将保存输出的文件的路径。	amass intel -o out.txt -whois -d example.com
-器官	要在 AS 语句中搜索的字符串表达式。	积累英特尔-org Facebook
-P	逗号分隔的端口号。	积累英特尔-cidr 104.154.0.0/15 -p 443,8080
-R	声明要在发现期间使用的 DNS 服务器。	积累英特尔 -r 8.8.8.8,1.1.1.1 -whois -d example.com
-RF	指示包含要在发现期间使用的 DNS 服务器列表的文件的路径。	amass intel -rf data/resolvers.txt -whois -d example.com
-SRC	指示从中获取发现的字段的来源。	amass intel -src -whois -d example.com
-暂停	发现期间要考虑的超时时间。	amass intel -timeout 30 -d example.com
-谁是	WHOIS 信息搜索其他类似域。	amass intel -whois -d example.com

积累枚举命令

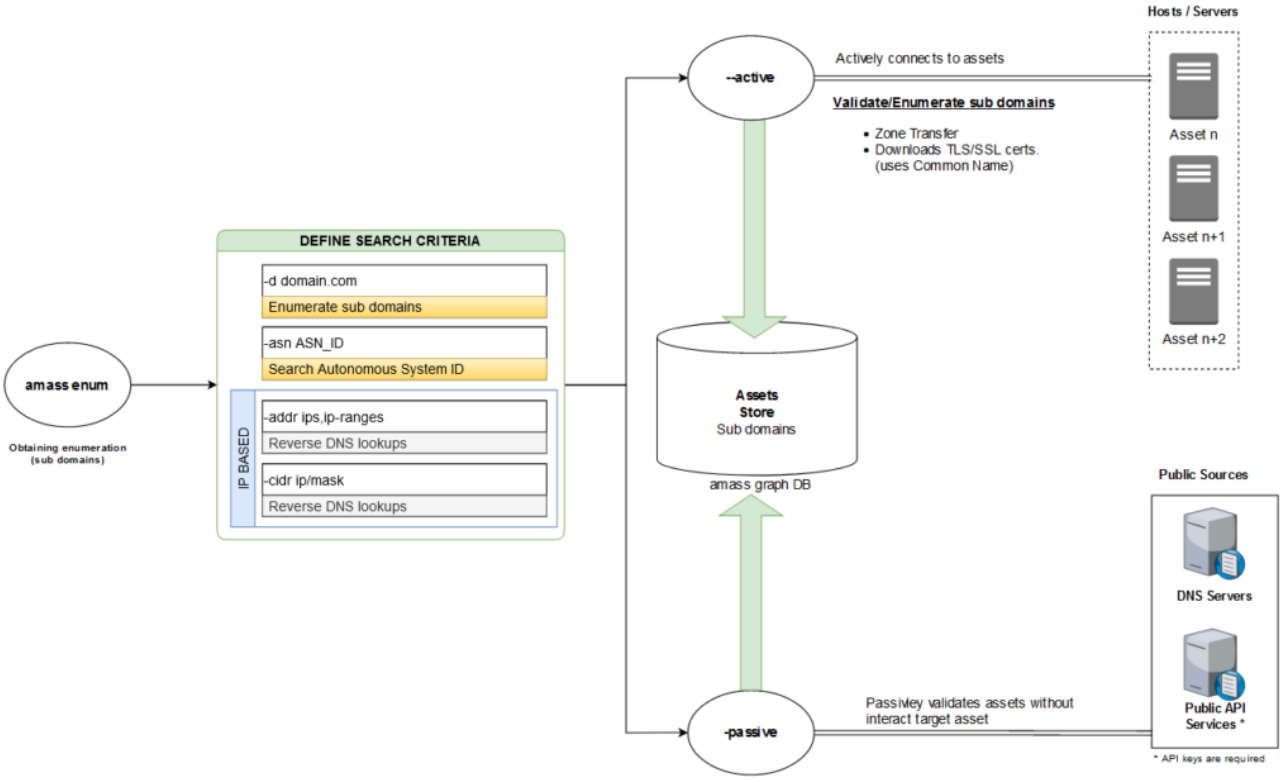
Amass 枚举可以在被动或主动模式下运行。被动模式要快得多，但 Amass 不会通过解析子域来验证 DNS 信息。您可以使用“-passive”标志被动地运行它，并且不能启用许多技术或配置，例如 DNS 解析和验证。有时需要选择被动模式而不是主动模式，例如：

- 因为您需要持续监控目标范围的更改，或者因为您正在进行网络钓鱼交互并搜索子域，所以您需要了解所有可能的子域已被使用并可能在未来被重用。
- 您可能需要在稍后阶段验证 DNS 信息并快速假脱机结果。
- 由于安全参与的限制或要求，您可能只需要执行被动信息收集。

要查看此子命令的可用选项，只需在终端中输入：

用法： amass enum [选项] -d DOMAIN

-积极的
尝试区域转移和证书名称抓取
-addr 值
IP 和范围 (192.168.1.1-254) 以逗号分隔
-d 值
域名以逗号分隔（可多次使用）
-cidr 值
以逗号分隔的 CIDR（可多次使用）
-asn 值
以逗号分隔的 ASN（可多次使用）



在下面的示例中，我们在 Owasp.org 上被动搜索子域，并要求 Amass 显示找到每个子域的数据源：

```
$ amass enum -passive -d owasp.org -src
[...]
[威胁人群] update-wiki.owasp.org
[...]
BufferOver] my.owasp.org
[ crtsh] www.lists.owasp.org
[ crtsh] www.ocms.owasp.org
[...]
查询 owasp.org 子域的 VirusTotal
查询 Yahoo 的 owasp.org 子域
[...]
```

此子命令将在探测时执行 DNS 发现和网络映射。此时值得注意的是， Amass 枚举将识别所有子域，尽管Amass intel 命令有助于收集 IP 范围、ASN 和组织拥有的主要域。

在主动配置模式下使用 Amass 意味着您将获得更准确的结果，并且可以发现更多资产，因为您可以启用所有 DNS 发现技术。在“启用配置模式”下，它将通过执行 SSL/TLS 服务的区域传输和端口扫描，从证书域（例如：Common Name）中搜索子域。

通常可以被认为是活动的，因为它在启用“-active”标志的情况下以多种方式（单词列表、掩码等）执行子域暴力破解。所有发现将由 Amass 使用默认或指定的分析器进行验证：

以下所有设置都与此子命令有关。以下标志可用于配置：

选择	*解释*	*样本*
-积极的	它使用主动方法。 Zone 尝试传输，连接到目标服务器以获取 SSL/TLS 证书。	amass enum -active -d example.com -p 80,443,8080
-aw	指示生成子域替代项的替代词文件的路径。	amass enum -aw PATH -d example.com
-bl	报告将不会被发现的子域的黑名单。	amass enum -bl blah.example.com -d example.com
-blf	使用列入黑名单的子域列表指定文件的路径。	amass enum -blf data/blacklist.txt -d example.com
-蛮	在子域探索中使用蛮力。	amass enum -brute -d example.com
-配置	指定 INI 配置文件的路径。	积累枚举-config config.ini
-D	用逗号分隔的字段名称。	amass enum -d example.com
-df	它从文件中提供根域。	积累枚举-df domain.txt
是	指定包含将存储扫描结果的数据库的目录的路径。	amass enum -dir PATH -d example.com
-ef	文件的路径，其中包含研究时不会使用的数据源列表。	amass enum -ef exclude.txt -d example.com
-排除	不会在扫描中使用的数据源列表。它通过用逗号分隔来指定。	amass enum -ef exclude.txt -d example.com
-如果	包含用于扫描的数据源列表的文件的路径。	amass enum -ef exclude.txt -d example.com
-包括	用于扫描的数据源列表。它以逗号分隔。	amass enum -include crtsh -d example.com

-绳索	它还显示已发现域的 IP 地址。	amass enum -ip -d example.com
-ipv4	它还显示已发现域的 IPv4 地址。	amass enum -ip -d example.com
-ipv6	它还显示已发现域的 IPv6 地址。	amass enum -ip -d example.com
-json	定义要以 JSON 格式保存的输出文件的路径。	amass enum -json out.json -d example.com
-列表	列出要在发现中使用的数据源。	amass 枚举列表
-日志	报告将记录错误的日志文件的路径。	amass enum -log amass.log -d example.com
-max-dns-查询	最大并发 DNS 查询数。	amass enum -max-dns-queries 200 -d example.com
-dns-qps	每秒跨所有域解析器（DNS 服务器）的最大 DNS 查询数。	amass enum -dns-qps 200 -d example.com
-rqps	每个不受信任的解析器每秒的最大 DNS 查询数。	amass enum -dns-qps 200 -d example.com
-trqps	每个受信任的解析器每秒的最大 DNS 查询数	amass enum -trqps 20 -d example.com
-min-for-recursive	在递归暴力破解之前看到的子域标签（默认值：1）	amass enum -brute -min-for-recursive 3 -d example.com
-最大深度	暴力破解的子域标签的最大数量	amass enum -brute -max-depth 3 -d example.com
-nf	提供已知子域的文件的路径（来自其他工具/来源）	amass enum -nf names.txt -d example.com
-noalts	禁用替代子域生成。	amass enum -noalts -d example.com
-norecursive	禁用递归蛮力。	amass enum -brute -norecursive -d example.com
-他	指定文本输出文件的路径。	amass enum -o out.txt -d example.com

-oA	用于命名所有输出文件的路径前缀。	amass enum -oA amass_scan -d example.com
-被动的	它执行完全被动的执行。	amass enum --passive -d example.com
-p	逗号分隔的端口号。	amass enum -d example.com -p 443,8080
-r	声明要在发现期间使用的 DNS 服务器。	amass enum -d example.com -p 443,8080
-en	受信任的 DNS 解析器的 IP 地址（可多次使用）	amass enum -en 8.8.8.8,1.1.1.1 -d example.com
-rf	指示包含要在发现期间使用的 DNS 服务器列表的文件的路径。	amass enum -en 8.8.8.8,1.1.1.1 -d example.com
-trf	指定提供受信任的 DNS 解析器的文件的路径。	amass enum -trf data/trusted.txt -d example.com
-src	指示从中获取发现的字段的来源。	amass enum -src -d example.com
-暂停	发现期间要考虑的超时时间。	amass enum -timeout 30 -d example.com
-w	报告不同单词列表文件的路径。	amass enum -brute -w wordlist.txt -d example.com

enum 命令最常见的用法如下。发出此命令后，amass 开始从互联网上搜索 meb.gov.tr 域名的子域。它询问它可以查询的所有数据源并返回一堆子域。

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

在此扫描中，在没有 DNS 解析的情况下执行（-被动）扫描。假设passive-config.ini 包含被动信息资源和API 密钥的列表。-passive 选项比 -active 返回更快但结果更少。

通过使用 -v 参数，您可以增加 amass.log 文件的详细程度，并在应用时更好地了解 amass 的特性。它允许您检测无法正常工作的数据源、查看阻止您的 IP 地址的服务以及无法正常工作的 DNS 解析器。

积累跟踪命令

为了监视目标的攻击面，它显示了对同一目标的侦察之间的差异。此子命令仅利用 'output_directory' 和配置文件中指定的远程数据库设置。

要查看此子命令的可用选项，只需在终端中输入：

用法：积累跟踪 [选项] -d 域
-d 值
域名以逗号分隔（可多次使用）
-历史
显示所有枚举对之间的差异
-最后一个整数
要包含在跟踪中的最近枚举数

选择	*解释*	*样本*
-配置	指定 INI 配置文件的路径。	积累轨道-config config.ini
-D	用逗号分隔的字段名称。	积累跟踪-d example.com
-df	它从文件中提供根域。	积累跟踪 -df 域.txt
是	指定包含存储扫描结果的数据库的目录的路径。	积累跟踪 -df 域.txt
-历史	它显示了发现之间的差异。	积累轨道历史
-最后的	要包含在跟踪中的最近发现的数量。	积累轨道-最后 2
-自从	排除指定日期之前的所有枚举（格式：01/02 15:04:05 2006 MST）	积累跟踪 - 自 DATE

amass track -d yahoo.com -last 2

上面的命令比较了域 yahoo.com 的最后两次扫描。

积累即命令

使用收集的信息创建可视化网络图。这种可视化对于解释返回综合结果的大型扫描中的实体之间的关系特别有用。此子命令仅利用配置文件中的"输出目录"和远程图形数据库设置。

为可视化创建的文件默认创建在当前工作目录中。以下是可用于将 DNS 和基础设施结果输出为网络图的开关：

选择	*解释*	*样本*
-配置	指定 INI 配置文件的路径。	积累即-config config.ini -d3
-D	用逗号分隔的字段名称。	amass viz -d3 -d example.com
-d3	生成 D3.js v4 格式的 HTML 模拟文件。	amass viz -d3 -d example.com
-df	定义包含根域的文件的路径。	amass viz -d3 -df domain.txt
是	定义包含 Graph 数据库的目录的路径。	amass viz -d3 -dir PATH -d example.com
-枚举	扫描结果通过数据库中的索引号识别发现。	amass viz -enum 1 -d3 -d example.com
-他	定义将保存输出文件的目录的路径。	amass viz -d3 -o OUTPATH -d example.com
-oA	定义输出文件的前缀。	amass viz -d3 -oA 示例 -d example.com
-gexf	输出图形交换 XML 格式 (GEXF) 格式。	amass viz -gexf -d example.com
-书法	Graphistry 返回 JSON 格式的输出。	amass viz -graphistry -d example.com
-maltego	输出 Maltego Graph Table 格式的 CSV 文件。	amass viz -maltego -d example.com

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

上述命令在带有关联图的 HTML 格式文件中显示域 yahoo.com 的所有结果。该图表是使用 d3 javascript 库创建的。使用 -o 选项， 输出将保存在 yahoo 目录中。vizz 命令还可以以 Maltego、XML 和 JSON 格式输出。

积累数据库命令

该命令允许您查看执行的每次扫描的发现数据。执行数据库的查看和处理。此子命令仅利用配置文件中的“输出目录”和远程数据库设置。与数据库中的勘探结果交互的使用选项包括：

选择	解释	样本
-配置	指定 INI 配置文件的路径。	积累 db -config config.ini
-D	用逗号分隔的字段名称。	amass db -d example.com
-DF	它从文件中提供根域。	积累 db -df 域.txt
是	指定包含扫描结果的数据库目录的路径。	amass db -dir 路径
-枚举	通过列表中的索引序列号检索发现信息。	amass db -enum 1 -显示
-进口	导入 JSON 格式的 amass 文件。	积累 db -import PATH
-绳索	它还显示已发现域的 IP 地址。	amass db -show -ip -d example.com
-IPV4	它还显示已发现域的 IPv4 地址。	amass db -show -ipv4 -d example.com
-IPV6	它还显示已发现域的 IPv6 地址。	amass db -show -ipv6 -d example.com
-JSON	定义要以 JSON 格式保存的输出文件的路径。	amass db -names -silent -json out.json -d example.com
-列表	列出要在发现中使用的数据源。	积累数据库列表
-名称	只带上发现的域。	amass db -names -d example.com
-无色	禁用颜色输出。	amass db -names -nocolor -d example.com
-他	指定文本输出文件的路径。	amass db -names -o out.txt -d example.com
-节目	打印结果发现目录 + 域的结果。	积累 db -show
-沉默的	在执行期间禁用所有输出。	amass db -names -silent -json out.json -d example.com
-SRC	指示从中获取发现的字段的来源。	amass db -show -src -d example.com
-概括	仅打印 ASN 表摘要。	amass db -summary -d example.com

要列出之前扫描的所有详细信息，只需运行 amass db -show即可查看当前结果，而无需重新扫描。如果您想查看特定域的详细信息，只需添加 -d 选项：

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

如果您喜欢漂亮、干净、简单的输出，您可以使用 -names 选项而不是 -show 来打印发现的域/子域。

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

显示在 amass4owasp 目录中注册的数据库中域名 owasp.org 的发现 #1 的结果。

生成 API 密钥

Amass 可以使用许多数据源。我在文章的开头列出了它们。但是，下面列出的数据源需要 API 密钥。

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

这些 API 密钥中的大多数都是免费的，但除非您拥有付费的 API 密钥，否则大多数只能提供有限的结果。免费的总比没有好。您需要找到上述各项服务的网站，然后注册并获取 API 密钥。这是一项非常耗时且乏味的任务，但好的发现并非没有牺牲。你可以这样做。获得所有 API 密钥后，将它们粘贴到 amass 配置文件中。有关全面的示例配置文件，请参见此

处。下面是一个配置文件的内容。那些写付费的人是有报酬的。使用示例文件中的 API 获取任何数据源，按如下方式添加它们并创建您自己的 amass 配置文件。然后使用名称 amass config.ini 保存文件，例如：

```
# https://passivedns.cn（联系方式）
[data_sources.360PassiveDNS]
[ data_sources.360PassiveDNS.Credentials ]
apikey = sizeozelapicode

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

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

现在，当您使用 amass 时，请使用 -config 参数指定配置文件，如下所示。这将增加您的 intel 和 enum 发现的数量和质量。我强烈建议您这样做，以便比其他人领先一步。

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

输出目录

amass 默认将上次扫描会话的日志和输出文件保存在 ~/.config/amass 下。进行新扫描时会重置这些文件。应在扫描结束时检查日志文件，因为它记录了扫描过程的进展情况和可能的错误。同样，扫描输出以 CSV 格式存储在此目录中。为每次扫描使用不同的存储库目录会很有用。您可以为此命令提供 -dir 选项。看看下面的例子：

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

使用上述命令，将搜索 ASN（自治网络）编号为 47524 的 TURKSAT 网络，并将发现保存在 turksat 目录中。

参考

Amass 项目网站： https :
//owasp-amass.com/ Amass 源代码： https ://github.com/OWASP/Amass
用户指南： https ://github.com/OWASP/Amass/blob/master/doc/ user_guide.md
使用示例： https ://github.com/OWASP/Amass/blob/master/doc/tutorial.md
Haklukes 的用户指南： https://hakluke.medium.com/haklukes-guide-to-amass-如何更有效地使用 amass-for-bug-bounties-7c37570b83f7

版权