OWASP накопить РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Автор : Озгюр Коджа, ozgurkoca.com, июнь 2022 г.

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

OWASP Amass выполняет сетевое картирование целей атаки и обнаружение внешних активов, используя методы сбора информации из открытых источников и активного обнаружения. Ознакомьтесь с методами , которые инструмент использует для поиска поддоменов , здесь. Amass , проект OWASP , является одним из важных инструментов blueteam , используемых в области разведки с открытым исходным кодом (OSINT) . Этот инструмент, написанный на языке Go , сфокусирован на анализе и обнаружении доменных имен.

Инструмент OWASP Amass получает поддомены путем очистки источников данных, рекурсивного перебора, сканирования веб-архивов, разрешения/изменения имен и обратного сканирования DNS. Кроме того, Amass использует IP-адреса, полученные во время разрешения, для обнаружения связанных сетевых блоков и ASN. Затем вся информация используется для создания карт целевых сетей. Методы исследований и открытий, которые использует Амасс, включают:

- **Модификация/перестановка** : примитивные изменения в найденных субдоменах (dev1 <-> dev2). Когда он видит поддомен, такой как customer1.domain.com, он также сканирует последовательные поддомены, такие как customer2.domain.com.
- **Нечеткий поиск по тегу/строке** : сложение и вычитание (dev <-> dav). Когда он видит поддомен, такой как dev.domain.com, он пытается найти возможные поддомены с простой заменой букв.

- **Рекурсивный брутфорс** : поиск API и WEB-архивов. Он ищет субдомены из таких архивов, как wayback.com и archiveit.com. Источники данных, которые он исследовал, перечислены ниже. Некоторые из них являются ограниченными службами, которым требуется ключ API.
- **Активные методы** : загрузка сертификатов HTTP TLS/SSL. Общее имя содержит информацию о субдомене.
- **Зоны** : Мониторинг перемещений по зонам и прохода по зонам (записи NSEC).
- **Общедоступные источники** : веб-архивы, pastebin, система контроля версий и веб-сайты социальных сетей.
- **Журналы прозрачности сертификатов (CT)** : CT — это платформа, используемая для отслеживания сертификатов и проверки того, является ли сертификат безопасным или вредоносным. Он пытается обнаружить, используя сертификаты, определенные для домена.
- **Заголовки HTTP CSP (политика безопасности контента)** : когда поддомены включены в политики, они заносятся в белый список, чтобы защитить их от атак CSS. Это создает источник данных для накопления в белых списках.

Ниже приведены источники данных, которые Amass использует для исследований и открытий. Вы можете запустить следующую команду, чтобы увидеть текущие источники данных и доступность amass.

```
накопить перечисление -список
```

Amass может использовать около 50 источников данных, некоторые из них бесплатные, некоторые с пробным использованием и некоторые довольно дорогие услуги. Вы можете добавить параметр -src к своим командам, чтобы отслеживать наиболее успешные источники данных. Таким образом, вы можете отслеживать, какой источник возвращает результаты и как часто.

ТЕХНИЧЕСКИЕ	ИСТОЧНИК ДАННЫХ
API	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
СЕРТИФИКАТЫ	Активные запросы (необязательно), Censys, CertSpotter, Crtsh, Digitorus, FacebookCT, GoogleCT
DNS	Брутфорс, обратная очистка DNS, обход зоны NSEC, перенос зоны, изменения/перестановки полных доменных имен, угадывание полных доменных имен на основе сходства
ОРИЕНТАЦИЯ	ARIN, BGPTools, BGPView, IPdata, IPinfo, NetworksDB, RADb, Robtex, ShadowServer, TeamCymru
СОСКОБ	ЗлоупотреблениеIPDB, Ask, Baidu, Bing, DNSDumpster, DuckDuckGo, Gists, HackerOne, HyperStat, IPv4Info, PKey, RapidDNS, Riddler, Searchcode, Searx, SiteDossier, Yahoo
ВЕБ-АРХИВЫ	AlienVault, AskDNS, DNSlytics, ONYPHE, SecurityTrails, SpyOnWeb, Umbrella, WhoisXMLAPI

ЗАПИСИ WHOIS	AlienVault, AskDNS, DNSlytics, ONYPHE, SecurityTrails, SpyOnWeb, Umbrella, WhoisXMLAPI

Amass — очень всеобъемлющий и продвинутый инструмент. Инструмент содержит 5 подкоманд: intel, enum, viz, track и db. **Командование** разведки проводит разведку цели. Полезно для установки отправной точки для пункта назначения. **enum** отображает цель для определения возможных точек атаки. **viz** помогает лучше анализировать, визуализируя полученные результаты. **track** используется для отслеживания и сравнения изменений цели с течением времени. amass сохраняет все разведывательные данные и результаты сканирования в собственной базе данных. Подкоманда **db** используется для доступа и запросов к этой базе данных. Вы можете обратиться к странице документа , чтобы получить доступ ко всем командам и параметрам накопления . В этой главе я приведу только основные примеры его использования.

Подкоманды накопления

- **собирать информацию** : обнаруживает корневые домены (не поддомены), ASN, выполняет обратные запросы WHOIS и DNS. Он проводит разведку из открытых источников для расследования целевой организации.
- **amass enum** : извлекает и сопоставляет записи DNS открытых систем с использованием поддоменов, быстрого режима (пассивного), обычного режима, методов разрешения/проверки DNS.
- **amass viz** : создает визуальную графику, удобную для визуального осмотра. Поддерживает Мальтего. Создает наглядную схему сделанных открытий и исследований.
- **Отслеживание накопления** : позволяет сравнить исторические данные между сканированиями и просмотром новых или обновленных активов.
- **db** : Amass хранит все активные и пассивные открытия в собственной базе данных. Команда db используется для доступа к этим записям позже.

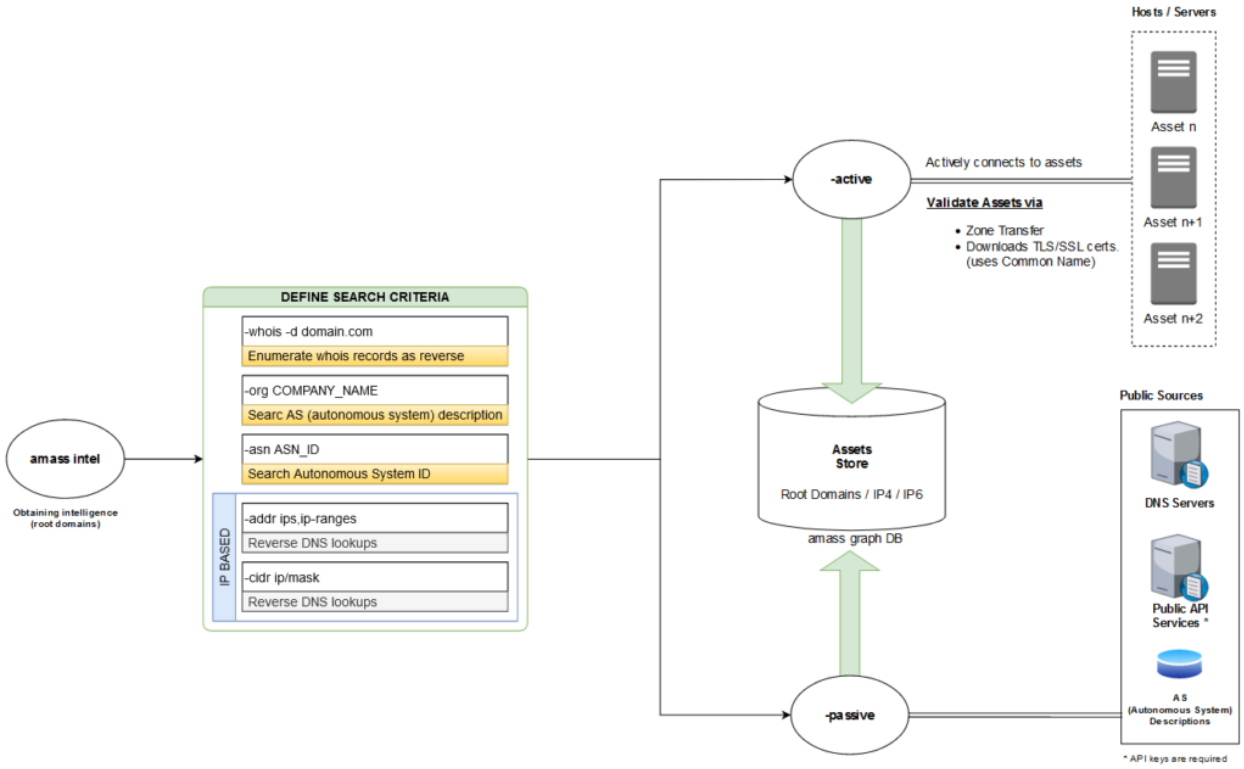
разведывательная команда

Подкоманда/модуль Amass intel может помочь собрать информацию из открытых источников о предприятии и позволит вам найти больше корневых доменных имен, связанных с предприятием. Чтобы увидеть доступные параметры для этой подкоманды, просто введите ее в терминал:

```
$ собирать информацию
[...]
Использование: собирать информацию [опции] [-whois -d ДОМЕН] [-addr ADDR -asn
ASN -cidr CIDR]
-активный
Попытка захвата имени сертификата
-адрес значение
```

```
IP-адреса и диапазоны (192.168.1.1-254), разделенные запятыми
-значение asn
ASN, разделенные запятыми (можно использовать несколько раз)
-cidr значение
CIDR, разделенные запятыми (можно использовать несколько раз)
-org строка
Строка поиска предоставлена по информации описания AS
-кто
Все предоставленные домены проходят через обратный whois
[...]
```

На данный момент стоит отметить, что еще одним большим преимуществом Amass является то, что все подкоманды пытаются поддерживать согласованность аргументов. В следующих абзацах включены параметры подкоманд , вы можете видеть, что большинство из них используются совместно. На приведенной ниже диаграмме в основном показана рабочая логика сбора информации.



По умолчанию эта подкоманда будет использовать набор методов сбора информации и источников данных, таких как WHOIS и IPv4Info, для получения организационной информации и родительских доменов, если это явно не отключено в файле конфигурации Amass. Пример файла конфигурации Amass доступен в [репозитории GitHub .]

```
$ собирать информацию -whois -d owasp.org
appseceu.com
owasp.com
appsecasiapac.com
appsecnorthamerica.com
appecus.com
[...]
owasp.org
```

```
appsecapac.com
appsecla.org
[...]
```

Вы также можете подтвердить некоторые из приведенных выше результатов, вручную просмотрев источники данных. На снимке экрана ниже мы выполнили обратный поиск Whois для «OWASP Foundation» и запросили у ViewDNS (также часть источников данных Amass) похожие домены:

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

При поиске с помощью Amass intel вы всегда можете запустить его с дополнительными параметрами конфигурации, например, вы можете попробовать передачу зоны с аргументом --active и подключить его к соответствующему серверу, чтобы получить сертификаты SSL/TLS для извлечения информации. Просто убедитесь, что у вас есть права на активный поиск цели, прежде чем делать это.

На данный момент стоит отметить, что некоторые флаги конфигурации не будут работать с другими, и в этом случае Amass их проигнорирует.

Выводы Amass не всегда могут быть точными по разным причинам, например, источники данных, используемые Amass, могут быть непоследовательными или неактуальными. Amass пытается дополнительно проверить информацию с помощью DNS-запросов. Несмотря на то, что Amass хорошо справляется со своей задачей, пользователям все же следует выполнять дополнительные проверки результатов, которые не кажутся соответствующими цели. Это может быть достигнуто с помощью различных методов, таких как:

- Используйте утилиты (например, dig, nslookup) для разрешения доменов.
- Выполните поиск в WHOIS, чтобы проверить сведения об организации.
- Используйте результаты поиска, такие как основные домены в поисковых системах.

```
накопить intel-org ТУРЦИЯ
```

Возвращает идентификаторы ASN, связанные со словом Турция. Этот тип поиска строк часто не дает достаточного количества результатов. Вы также можете добавить ключ -active, если хотите, чтобы поиск выполнялся также с использованием активных методов. Приведенная выше команда будет искать Турцию в описаниях ASN и возвращать связанные ASN.

Ключ org ищет идентификаторы ASN (автономная система), связанные с данным выражением. Строка, указанная с параметром -org, ищется в записях AS и находится ее идентификатор ASN. ASN ID — это номер автономной системы, присвоенный Управлением по присвоению номеров в Интернете (IANA), он представлен уникальным во всем мире 16-значным идентификационным номером. AS (автономная система) относится к большой сети или группе сетей с единой политикой маршрутизации (rfc1930). Идентифицирует их в идентификаторе ASN. Например, номер ASN сети TTNET — 9121, CloudFlare — 13335, ULAKNET — 8517 и Amazon — 16509. Большие маршрутизаторы используют эти номера ASN, когда необходимо выполнить маршрутизацию между сетями.

Теперь попробуем найти доменные имена в найденном нами ASN. Проверьте команду ниже.

```
собрать информацию -active -src -ip -asn 8517 -p 80 443
```

Он выполнит обнаружение с использованием активных методов (-active) на портах 80 и 443 доменов в автономной сети (ULAKNET) с номером ASN 8517. Он будет использовать сертификаты TLS/SSL для активного обнаружения. amass извлечет SSL-сертификат, который будет подключаться ко всем IP-адресам указанного ASN, и перечислит домен, с которым связан SSL-сертификат. Он также будет отображать источники (-src) и IP-адреса (-ip) найденных доменов.

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

Диапазон строк объявляется с параметром -cidr. Число 24 представляет сетевую маску и соответствует 255.255.255.0. amass будет искать и обнаруживать различные источники IP-адресов между 193.140.28.1 и 193.140.28.254, обнаруживая и перечисляя доменные имена, направленные на эти IP-адреса. Кроме того, активное обнаружение будет осуществляться с использованием сертификатов TLS/SSL для портов 80 и 443. Он будет подключаться к каждому IP-адресу, извлекать SSL-сертификаты и перечислять доменные имена, упомянутые в сертификате.

```
накопить Intel -активный -ip -src -cidr 74.6.0.6/16 -addr 74.6.231.20-21 -p
80.8080
```

Он будет сканировать компьютеры в сети 74.6.0.6/16, используя активные методы. В нем будут перечислены IP-адреса и источники найденных доменов. Он будет выполнять обратный DNS-запрос на компьютерах в диапазоне 74.6.231.20-21.

```
собирать информацию - whois -d yahoo.com
```

Он пытается найти доменные имена путем обратного поиска в записях WHOIS данного домена (-d) или в списке доменов (-df). В этом примере amass обращается к записям WHOIS

сайта yahoo.com и пытается найти корневые домены других организаций, которые могут совпадать с этими записями WHOIS. Это полезно для поиска других доменов, принадлежащих организации/компании, но записи WHOIS не всегда могут содержать точную информацию или сохранять конфиденциальность.

```
собрать информацию -asn 8517 -whois -d omu.edu.tr
```

Эта команда ищет другие домены с такими же WHOIS-записями в автономной сети ULAKNET с ASN ID 8517.

Ниже приведена таблица, показывающая параметры и области использования команды intel.

ВЫБОР	ОБЪЯСНЕНИЕ	ОБРАЗЕЦ
-АКТИВНЫЙ	Он использует активные методы. Zone пытается выполнить передачу, подключается к целевому серверу для получения сертификатов SSL/TLS.	собрать информацию -active -addr 192.168.2.1-64 -p 80 443 8080
-АДРЕС	Указывает диапазоны IP-адресов. Диапазоны разделяются запятыми.	192.168.2.1-64,192.168.3.10-254
-АСН	Сообщает идентификатор ASN. ASN ID — это уникальный номер, присваиваемый IANNA крупным компьютерным сетям.	собрать информацию -ASN 13374,14618
-СИДР	Определяет сеть. Число после косой черты определяет сетевую маску.	собрать информацию -cidr 104.154.0.0/15
-CONFIG	Указывает расположение файла конфигурации сканирования.	собрать информацию -config config.ini
-Д	Имена полей, разделенные запятыми.	собирать информацию -whois -d example.com
-ДФ	Он загружает корневые домены из файла.	собрать информацию -whois -df domains.txt
ЯВЛЯЕТСЯ	Указывает путь к каталогу, содержащему базу данных, в которой будут храниться результаты сканирования.	собрать информацию -dir ПУТЬ -cidr 104.154.0.0/15
-ЭФ	Путь к файлу со списком источников данных, которые не будут использоваться при исследовании.	собрать информацию -whois -ef exclude.txt -d example.com
-ИСКЛЮЧИТЬ	Список источников данных, которые не будут использоваться при сканировании. Он указывается через запятую.	собрать информацию -whois -exclude crtsh -d example.com

-ЕСЛИ	Путь к файлу со списком источников данных для сканирования.	собрать информацию -whois -if include.txt -d example.com
-ВКЛЮЧАЮТ	Список источников данных для сканирования. Пишется через запятую.	собирать информацию -whois -include crtsh -d example.com
-ВЕРЕВКА	Он также показывает IP-адреса обнаруженных доменов.	собирать информацию -ip -whois -d example.com
-IPV4	Он также показывает IPv4-адреса обнаруженных доменов.	собрать информацию -ipv4 -whois -d example.com
-IPV6	Он также показывает IPv6-адреса обнаруженных доменов.	собрать информацию -ipv6 -whois -d example.com
-СПИСОК	Список источников данных для использования при обнаружении.	собирать информацию -список
-ЖУРНАЛ	Сообщает путь к файлу журнала, в который будут записываться ошибки.	собирать информацию -log amass.log -whois -d example.com
-MAX-DNS-ЗАПРОСЫ	Максимальное количество одновременных DNS-запросов.	собрать информацию -max-dns-queries 200 -whois -d example.com
-ОН	Путь к файлу, в котором будут сохранены выходные данные.	собирать информацию -o out.txt -whois -d example.com
-ОРГАН	Строковое выражение для поиска в операторе AS.	собирать информацию -org Facebook
-П	Номера портов, разделенные запятыми.	собрать информацию -cidr 104.154.0.0/15 -p 443,8080
-Р	Объявляет DNS-серверы, которые будут использоваться во время обнаружения.	собрать информацию -r 8.8.8.8,1.1.1.1 -whois -d example.com
-РФ	Указывает путь к файлу, содержащему список DNS-серверов, которые будут использоваться во время обнаружения.	собирать информацию -rf data/resolvers.txt -whois -d example.com
-ИСТОЧНИК	Указывает источник, из которого были получены обнаруженные поля.	собрать информацию -src -whois -d example.com
-ТАЙМ-АУТ	Период тайм-аута, который следует учитывать при обнаружении.	собрать информацию -timeout 30 -d example.com
-КТО	Информация WHOIS ищет другие подобные домены.	собирать информацию -whois -d example.com

команда перечисления

Перечисление Amass может работать в пассивном или активном режиме. Пассивный режим намного быстрее, но Amass не будет проверять информацию DNS путем разрешения поддоменов. Вы можете запустить его пассивно, используя флаг «-passive», и не можете

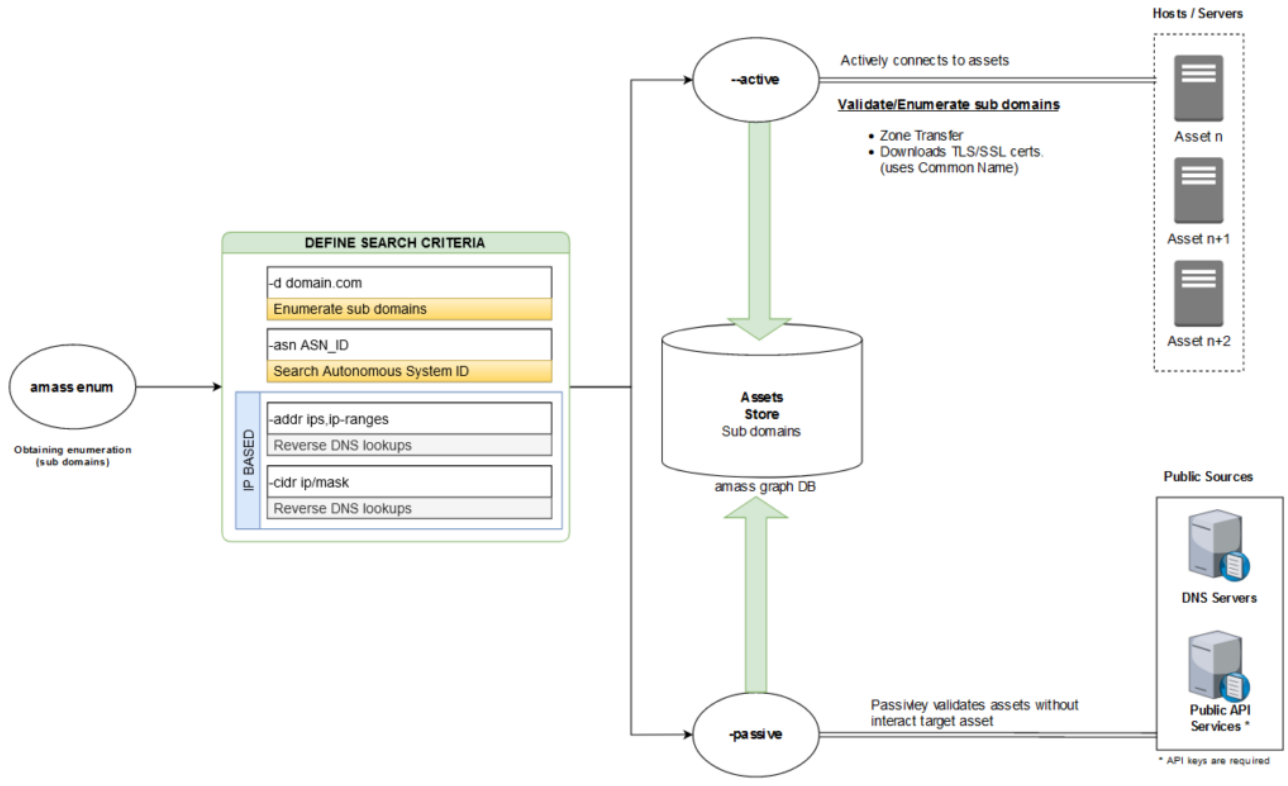
включить многие методы или конфигурации, такие как разрешение и проверка DNS. Иногда необходимо выбрать пассивный режим вместо активного, например:

- Поскольку вам необходимо постоянно отслеживать целевую область на наличие изменений или поскольку вы работаете над фишинговым взаимодействием и ищете субдомены, вам необходимо знать все возможные субдомены, которые использовались и могут быть повторно использованы в будущем.
- Возможно, вам потребуется проверить информацию DNS на более позднем этапе и быстро спулировать результаты.
- Из-за ограничений или требований по обеспечению безопасности вам может потребоваться только пассивный сбор информации.

Чтобы увидеть доступные параметры для этой подкоманды, просто введите ее в терминал:

```
Использование: enum enum [параметры] -d ДОМЕН

-активный
Попытка передачи зоны и захвата имени сертификата
-адрес значение
IP-адреса и диапазоны (192.168.1.1-254), разделенные запятыми
-d значение
Доменные имена, разделенные запятыми (можно использовать несколько раз)
-cidr значение
CIDR, разделенные запятыми (можно использовать несколько раз)
-значение asn
ASN, разделенные запятыми (можно использовать несколько раз)
```



В приведенном ниже примере мы пассивно ищем поддомены на Owasp.org и просим Amass показать источники данных, в которых он находит каждый поддомен:

```
$ накопить 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
[...]
Запрос VirusTotal для субдоменов owasp.org
Запрос Yahoo для субдоменов owasp.org
[...]
```

Эта подкоманда выполнит обнаружение DNS и сопоставление сети во время проверки. Здесь стоит отметить , что перечисление Amass идентифицирует все поддомены, хотя команда Amass intel помогает собирать диапазоны IP-адресов, номера ASN и основные домены, принадлежащие организации.

Использование Amass в режиме активной конфигурации означает, что вы получите более точные результаты и сможете обнаружить больше ресурсов, поскольку вы можете включить все методы обнаружения DNS. При «включенном режиме конфигурации» он будет искать поддомены из доменов сертификатов (например, «Общее имя») , выполняя передачу зоны и сканирование портов служб SSL/TLS .

в целом может считаться активной, поскольку она выполняет перебор субдоменов несколькими способами (список слов, маски и т. д.) с включенным флагом «-active» . Все результаты будут проверены Amass с использованием анализаторов по умолчанию или указанных:

Все приведенные ниже настройки относятся к этой подкоманде. Для настройки доступны следующие флаги:

Выбор	***Объяснение***	***Образец***
-активный	Он использует активные методы. Zone пытается выполнить передачу, подключается к целевому серверу для получения сертификатов SSL/TLS.	накопить enum -active -d example.com -p 80 443 8080
-ау	Указывает путь к альтернативному файлу слов для создания альтернатив поддоменов.	накопить enum -aw ПУТЬ -d example.com
-бл	Сообщает о черном списке поддоменов, которые не будут обнаружены.	накопить перечисление -bl blah.example.com -d example.com
-блф	Указывает путь к файлу со списком занесенных в черный список субдоменов.	накопить enum -blf data/blacklist.txt -d example.com
-грубый	Использует грубую силу при исследовании поддоменов.	накопить enum -brute -d example.com
-config	Указывает путь к файлу конфигурации INI.	накопить enum -config config.ini

-Д	Имена полей, разделенные запятыми.	накопить enum -d example.com
-дф	Он загружает корневые домены из файла.	накопить enum -df domains.txt
является	Указывает путь к каталогу, содержащему базу данных, в которой будут храниться результаты проверки.	накопить enum -dir PATH -d example.com
-эф	Путь к файлу со списком источников данных, которые не будут использоваться при исследовании.	накопить enum -ef exclude.txt -d example.com
-исключать	Список источников данных, которые не будут использоваться при сканировании. Он указывается через запятую.	накопить enum -ef exclude.txt -d example.com
-если	Путь к файлу со списком источников данных для сканирования.	накопить enum -ef exclude.txt -d example.com
-включают	Список источников данных для сканирования. Пишется через запятую.	накопить enum -include crtsh -d example.com
-веревка	Он также показывает IP-адреса обнаруженных доменов.	накопить enum -ip -d example.com
-ipv4	Он также показывает IPv4-адреса обнаруженных доменов.	накопить enum -ip -d example.com
-ipv6	Он также показывает IPv6-адреса обнаруженных доменов.	накопить enum -ip -d example.com
-json	Определяет путь к выходному файлу, который будет сохранен в формате JSON.	накопить перечисление -json out.json -d example.com
-список	Список источников данных для использования при обнаружении.	накопить перечисление -список
-журнал	Сообщает путь к файлу журнала, в который будут записываться ошибки.	накопить enum -log накопить.log -d example.com
-max-dns-запросы	Максимальное количество одновременных DNS-запросов.	накопить enum -max-dns-queries 200 -d example.com
-dns-qps	Максимальное количество DNS-запросов в секунду для всех преобразователей домена (DNS-сервер).	накопить enum -dns-qps 200 -d example.com
-rqps	Максимальное количество DNS-запросов в секунду для каждого ненадежного преобразователя.	накопить enum -dns-qps 200 -d example.com
-trqps	Максимальное количество DNS-запросов в секунду для каждого доверенного распознавателя	накопить enum -trqps 20 -d example.com
-мин-для-рекурсивного	Метки поддоменов, видимые перед рекурсивным подбором (по умолчанию: 1)	накопить enum -brute -min-for-recursive 3 -d example.com

-Максимальная глубина	Максимальное количество тегов поддоменов для перебора	накопить enum -brute -max-depth 3 -d example.com
-нф	Путь к файлу с уже известными субдоменами (из других инструментов/источников)	накопить enum -nf имена.txt -d example.com
-нет	Отключает альтернативную генерацию поддоменов.	накопить enum -noalts -d example.com
-норекурсивный	Отключает рекурсивный брутфорс.	накопить enum -brute -norecursive -d example.com
-Он	Указывает путь к текстовому выходному файлу.	накопить enum -o out.txt -d example.com
-оА	Префикс пути, используемый для обозначения всех выходных файлов.	накопить enum -oA amass_scan -d example.com
-пассивный	Он выполняет полностью пассивное исполнение.	накопить перечисление --passive -d example.com
-п	Номера портов, разделенные запятыми.	накопить enum -d example.com -p 443,8080
-р	Объявляет DNS-серверы, которые будут использоваться во время обнаружения.	накопить enum -d example.com -p 443,8080
-ен	IP-адреса доверенных DNS-преобразователей (можно использовать несколько раз)	накопить перечисление -en 8.8.8.8,1.1.1.1 -d example.com
-рф	Указывает путь к файлу, содержащему список DNS-серверов, которые будут использоваться во время обнаружения.	накопить перечисление -en 8.8.8.8,1.1.1.1 -d example.com
-trf	Указывает путь к файлу, который предоставляет доверенные преобразователи DNS.	накопить перечисление -trf data/trusted.txt -d example.com
-источник	Указывает источник, из которого были получены обнаруженные поля.	накопить enum -src -d example.com
-тайм-аут	Период тайм-аута, который следует учитывать при обнаружении.	накопить enum -timeout 30 -d example.com
-w	Сообщает путь к другому файлу списка слов.	накопить enum -brute -w wordlist.txt -d example.com

Наиболее часто команда enum используется следующим образом. После подачи этой команды система начинает поиск поддоменов доменного имени meb.gov.tr из Интернета. Он запрашивает все возможные источники данных и возвращает стек субдоменов.

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

В этом сканировании (-пассивное) сканирование выполняется без разрешения DNS. Предположим, что файлpassive-config.ini содержит список пассивных информационных ресурсов и ключей API. Опция -passive возвращает быстрее, но меньше результатов, чем -active.

Используя параметр -v, вы можете повысить уровень детализации файла amass.log и лучше понять особенности amass при его применении. Это позволяет вам обнаруживать источники данных, которые не работают должным образом, видеть службы, которые блокируют ваш IP-адрес, и преобразователи DNS, которые не работают должным образом.

собрать команду отслеживания

Чтобы контролировать поверхность атаки цели, он показывает различия между разведкой одной и той же цели (целей). Эта подкоманда использует только «output_directory» и настройки удаленной базы данных, указанные в файле конфигурации.

Чтобы увидеть доступные параметры для этой подкоманды, просто введите ее в терминал:

```
Использование: накапливать трек [параметры] -d домен
-d значение
Доменные имена, разделенные запятыми (можно использовать несколько раз)
-история
Показать разницу между всеми парами перечисления
-последний интервал
Количество последних перечислений для включения в отслеживание
```

Выбор	***Объяснение***	***Образец***
-config	Указывает путь к файлу конфигурации INI.	собрать трек -config config.ini
-Д	Имена полей, разделенные запятыми.	накапливать трек -d example.com
-дф	Он загружает корневые домены из файла.	собрать трек -df domains.txt
является	Указывает путь к каталогу, содержащему базу данных, в которой хранятся результаты сканирования.	собрать трек -df domains.txt
-история	Он показывает различия между открытиями.	накопить трек-история
-последний	Количество недавних открытий для включения в отслеживание.	Накопить трек -последние 2
-поскольку	Исключить все перечисления до указанной даты (формат: 02.01 15:04:05 2006 MST)	собирать трек – с DATE

```
собрать трек -d yahoo.com -последние 2
```

Приведенная выше команда сравнивает два последних сканирования домена yahoo.com.

собрать, а именно команду

Создает визуальные сетевые графики, используя собранную информацию. Эта визуализация особенно полезна для интерпретации взаимосвязей между объектами в больших сканах, которые возвращают исчерпывающие результаты. Эта подкоманда использует только настройки «output_directory» и удаленной графической базы данных из файла конфигурации.

Файлы, созданные для визуализации, по умолчанию создаются в текущем рабочем каталоге. Вот переключатели, которые можно использовать для вывода результатов DNS и инфраструктуры в виде сетевых графов:

Выбор	***Объяснение***	***Образец***
-config	Указывает путь к файлу конфигурации INI.	собрать, а именно -config config.ini -d3
-Д	Имена полей, разделенные запятыми.	накопить, а именно -d3 -d example.com
-d3	Создает файл моделирования HTML в формате D3.js v4.	накопить, а именно -d3 -d example.com
-дф	Определяет путь к файлу, содержащему корневые домены.	собрать, а именно -d3 -df domains.txt
является	Определяет путь к каталогу, содержащему базу данных Graph.	накопить, а именно -d3 -dir ПУТЬ -d example.com
-перечисление	Результаты сканирования идентифицируют обнаружение по его порядковому номеру в базе данных.	накопить, а именно -enum 1 -d3 -d example.com
-Он	Определяет путь к каталогу, в котором будут сохранены выходные файлы.	накопить, а именно -d3 -o OUTPATH -d example.com
-оА	Определяет префикс для выходных файлов.	накапливать, а именно -d3 -oA пример -d example.com
-gexf	Выходные данные Graph Exchange XML Format (GEXF) отформатированы.	накопить, а именно -gexf -d example.com
-графика	Graphistry возвращает выходные данные в формате JSON.	накопить, а именно -graphistry -d example.com
-мальтего	Выводит CSV-файл в формате таблицы графиков Maltego.	накопить, а именно -maltego -d example.com

```
накапливать, а именно -d yahoo.com -d3 -o yahoo
```

Приведенная выше команда отображает все результаты для домена yahoo.com в файле в формате HTML с ассоциативным графом. Диаграмма создается с помощью javascript-библиотеки d3 . С опцией -o вывод сохраняется в каталоге yahoo. Команда vizz также может выводить данные в форматах Maltego, XML и JSON.

собрать команду БД

Это команда, которая позволяет просматривать данные обнаружения для каждого выполненного сканирования. Выполняет просмотр и обработку базы данных. Эта

подкоманда использует только настройки «output_directory» и удаленной базы данных из файла конфигурации. Варианты использования для взаимодействия с результатами разведки в базе данных:

ВЫБОР	ОБЪЯСНЕНИЕ	ОБРАЗЕЦ
-CONFIG	Указывает путь к файлу конфигурации INI.	собрать базу данных -config config.ini
-Д	Имена полей, разделенные запятыми.	накопить db -d example.com
-ДФ	Он загружает корневые домены из файла.	накопить db -df domains.txt
ЯВЛЯЕТСЯ	Указывает путь к каталогу базы данных, содержащему результаты сканирования.	накопить db -dir ПУТЬ
-ПЕРЕЧИСЛЕНИЕ	Извлекает информацию об обнаружении через порядковый номер индекса из списка.	собрать базу данных -enum 1 -show
-ИМПОРТ	Импортирует файл накопления в формате JSON.	накопить БД -импорт ПУТЬ
-ВЕРЕВКА	Он также показывает IP-адреса обнаруженных доменов.	накопить базу данных -show -ip -d example.com
-IPV4	Он также показывает IPv4-адреса обнаруженных доменов.	накопить базу данных -show -ipv4 -d example.com
-IPV6	Он также показывает IPv6-адреса обнаруженных доменов.	накопить базу данных -show -ipv6 -d example.com
-JSON	Определяет путь к выходному файлу, который будет сохранен в формате JSON.	накопить db -names -silent -json out.json -d example.com
-СПИСОК	Список источников данных для использования при обнаружении.	накопить БД -список
-ИМЕНА	Приводите только открытые домены.	накопить db -names -d example.com
-НЕТ ЦВЕТА	Отключает цветной вывод.	накопить базу данных -names -nocolor -d example.com
-ОН	Указывает путь к текстовому выходному файлу.	накопить базу данных -names -o out.txt -d example.com
-ПОКАЗЫВАТЬ	Выводит результаты для полученного каталога обнаружения + домены.	накопить БД-шоу
-ТИХИЙ	Отключает весь вывод во время выполнения.	накопить db -names -silent -json out.json -d example.com
-ИСТОЧНИК	Указывает источник, из которого были получены обнаруженные поля.	накопить базу данных -show -src -d example.com
-РЕЗЮМЕ	Печатает только сводку таблицы ASN.	накопить базу данных -summary -d example.com

Чтобы получить список всех деталей ваших предыдущих сканирований, просто запустите amass db -show , чтобы вы могли видеть текущие результаты без необходимости нового сканирования. Если вы хотите просмотреть сведения о конкретном домене, просто добавьте параметр -d:

```
накопить базу данных -show -d paypal.com
```

Если вы предпочитаете красивый, чистый и простой вывод, вы можете распечатать обнаруженные домены/поддомены, используя опцию -names вместо -show.

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

Отображает результаты обнаружения №1 доменного имени owasp.org в базе данных, зарегистрированной в каталоге amass4owasp.

Генерация ключей API

Существует множество источников данных, которые может использовать Amass. Их список я привел в начале статьи. Однако для перечисленных ниже источников данных требуется ключ API.

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

Большинство этих ключей API бесплатны, но большинство из них дают ограниченные результаты, если у вас нет платного ключа API. Бесплатные лучше, чем ничего. Вам нужно будет найти веб-сайт для каждой из вышеперечисленных служб, затем зарегистрироваться и получить ключ API. Это очень трудоемкая и утомительная задача, но хорошее открытие не приходит без жертв. Ты можешь это сделать. Когда у вас есть все ваши API-ключи, вставьте их в файл конфигурации amass. См. здесь полный пример файла конфигурации . Ниже приведено содержимое файла конфигурации. Тем, кто пишет Paid, платят. Получите любой из источников данных с помощью API в образце файла, добавьте их следующим образом и создайте собственный файл конфигурации для накопления. Затем сохраните файл с именем amassconfig.ini, например:

```
# https://passivedns.cn (Контакты)
[data_sources.360PassiveDNS]
[ источники_данных.360PassiveDNS.Учетные данные ]
apikey = размерозелапикод
```

```
# https://ahrefs.com (платно)
[ источники_данных.Ahrefs ]
ттл = 4320
[ источники_данных.Ahrefs.Учетные данные ]
apikey = размерозелапикод

# https://otx.alienvault.com (бесплатно)
[ источники_данных.AlienVault ]
[ источники_данных.AlienVault.Credentials ]
apikey = размерозелапикод
```

Теперь, когда вы используете накопление, укажите файл конфигурации с параметром -config следующим образом. Это повысит количество и качество ваших открытий разведданных и перечислений. Я настоятельно рекомендую вам сделать это, чтобы быть на шаг впереди других.

```
накопить перечисление -d turkiye.gov.tr -config ./amasconfig.ini
```

выходной каталог

По умолчанию amass хранит журнал и выходные файлы для последнего сеанса сканирования в ~/.config/amass. Эти файлы сбрасываются при выполнении нового сканирования. Файл журнала следует проверять в конце сканирования, так как в нем фиксируется ход процесса сканирования и возможные ошибки. Точно так же результаты сканирования сохраняются в этом каталоге в формате CSV. Может быть полезно использовать разные каталоги репозитория для каждого сканирования. Для этого вы можете указать параметр -dir для команды. Посмотрите пример ниже:

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

С помощью приведенной выше команды будет выполнен поиск в сети TURKSAT с номером ASN (автономная сеть) 47524, и обнаруженные данные будут сохранены в каталоге turksat.

использованная литература

Веб-сайт проекта Amass: https://owasp-amass.com/
Исходный код Amass: https://github.com/OWASP/Amass
Руководство пользователя: https://github.com/OWASP/Amass/blob/master/doc/user_guide.md
Примеры использования: https://github.com/OWASP/Amass/blob/master/doc/tutorial.md
Руководство пользователя Haklukes: https://hakluke.medium.com/haklukes-guide-to-amass-как использовать-накопить-более эффективно-для-баунти-7c37570b83f7

Авторские права