OWASP amasar MANUAL DE USUARIO

Autor : Özgür Koca, ozgurkoca.com, junio de 2022

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

OWASP Amass realiza un mapeo de red de objetivos de ataque y descubrimiento de activos externos utilizando técnicas de descubrimiento activo y recopilación de información de código abierto. Consulte las técnicas que utiliza la herramienta para encontrar subdominios aquí. Amass , un proyecto de OWASP , es una de las herramientas importantes de blueteam utilizadas en el campo de la inteligencia de fuente abierta (OSINT) . Escrito en el lenguaje Go , el enfoque principal de la herramienta es la inteligencia y el descubrimiento de nombres de dominio.

La herramienta OWASP Amass obtiene subdominios raspando fuentes de datos, fuerza bruta recursivamente, escaneando archivos web, permitiendo/cambiando nombres y escaneando DNS inverso. Además, Amass usa direcciones IP obtenidas durante la resolución para descubrir bloques de red asociados y ASN. Luego, toda la información se utiliza para crear mapas de redes de destino. Las técnicas de investigación y descubrimiento que utiliza Amass incluyen:

- **Modificación/Permutación** : Cambios primitivos a los subdominios encontrados (dev1 <-> dev2). Cuando ve un subdominio como cliente1.dominio.com, también analiza subdominios secuenciales como cliente2.dominio.com.
- **Búsqueda difusa de etiquetas/cadenas** : Suma resta (dev <-> dav). Cuando ve un subdominio como dev.domain.com, intenta encontrar posibles subdominios con simples cambios de letra.
- **Fuerza bruta recursiva** : búsqueda de APIs y archivos WEB. Busca subdominios de archivos como wayback.com y archiveit.com. Las fuentes de datos que exploró se

enumeran a continuación. Algunos de estos son servicios limitados que necesitan una clave API.

- **Técnicas activas** : Descarga de certificados HTTP TLS/SSL. Nombre común contiene información de subdominio.
- **Zonas** : Monitoreo de transferencias de zona y caminata de zona (registros NSEC).
- **Fuentes públicas** : archivos web, pastebin, control de versiones y sitios web de redes sociales.
- **Registros de Certificate Transparancey (CT)** : CT es un marco utilizado para rastrear certificados y verificar si un certificado es seguro o malicioso. Intenta descubrir utilizando los certificados definidos para el dominio.
- **Encabezados HTTP CSP (política de seguridad de contenido)** : cuando los subdominios se incluyen en las políticas, se incluyen en la lista blanca aquí para protegerlos de los ataques de CSS. Esto crea una fuente de datos para acumular en listas blancas.

A continuación se encuentran las fuentes de datos que Amass utiliza para la investigación y el descubrimiento. Puede ejecutar el siguiente comando para ver las fuentes de datos actuales y la disponibilidad de amass.

```
amasar enumeración -lista
```

Amass puede usar alrededor de 50 fuentes de datos, algunas de ellas gratuitas, otras con uso de prueba y algunas con servicios bastante costosos. Puede agregar el parámetro -src a sus comandos para realizar un seguimiento de las fuentes de datos más exitosas. Para que pueda realizar un seguimiento de qué fuente devuelve resultados y con qué frecuencia.

TÉCNICO	FUENTE DE DATOS
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
CERTIFICADOS	Extracciones activas (opcional), Censys, CertSpotter, Crtsh, Digitorus, FacebookCT, GoogleCT
DNS	Fuerza bruta, barrido de DNS inverso, caminata de zona NSEC, transferencias de zona, alteraciones/permutaciones de FQDN, adivinación basada en similitud de FQDN
ORIENTACIÓN	ARIN, BGPTools, BGPView, IPdata, IPinfo, NetworksDB, RADb, Robtex, ShadowServer, TeamCymru
RASPADO	AbuseIPDB, Ask, Baidu, Bing, DNSDumpster, DuckDuckGo, Gists, HackerOne, HyperStat, IPv4Info, PKey, RapidDNS, Riddler, Searchcode, Searx, SiteDossier, Yahoo
ARCHIVOS WEB	AlienVault, AskDNS, DNSlytics, ONYPHE, SecurityTrails, SpyOnWeb, Umbrella, WhoisXMLAPI
REGISTROS WHOIS	AlienVault, AskDNS, DNSlytics, ONYPHE, SecurityTrails, SpyOnWeb, Umbrella, WhoisXMLAPI

Amass es una herramienta muy completa y avanzada. La herramienta contiene 5 subcomandos, intel, enum, viz, track y db. El comando de **inteligencia hace un reconocimiento del objetivo.** Útil para establecer un punto de partida para el destino. **enum** mapea el objetivo para identificar posibles puntos de ataque. a **saber** , ayuda en un mejor análisis al visualizar los resultados obtenidos. **track** se utiliza para rastrear y comparar cambios a lo largo del tiempo en el objetivo. amass guarda todos los resultados de análisis e inteligencia en su propia base de datos. El subcomando **db se** utiliza para acceder y consultar esta base de datos. Puede consultar la página del documento para acceder a todos los comandos y opciones de amass . En este capítulo, solo ejemplificaré sus usos básicos.

Amasar subcomandos

- **acumular información** : descubre dominios raíz (no subdominios), ASN, realiza consultas inversas de WHOIS y DNS. Lleva a cabo inteligencia de código abierto para la investigación de la organización objetivo.
- **amass enum** : extrae y mapea registros DNS de sistemas abiertos utilizando subdominios, modo rápido (pasivo), modo normal, técnicas de resolución/validación de DNS.
- **amass viz** : crea gráficos visuales, buenos para la inspección visual. Apoya Maltego. Crea un diagrama visual de los descubrimientos e investigaciones realizadas.
- **amass track** : permite la comparación histórica entre escaneos y la visualización de activos nuevos o actualizados.
- **db** : Amass almacena todos los descubrimientos activos y pasivos en su propia base de datos. El comando db se usa para acceder a estos registros más adelante.

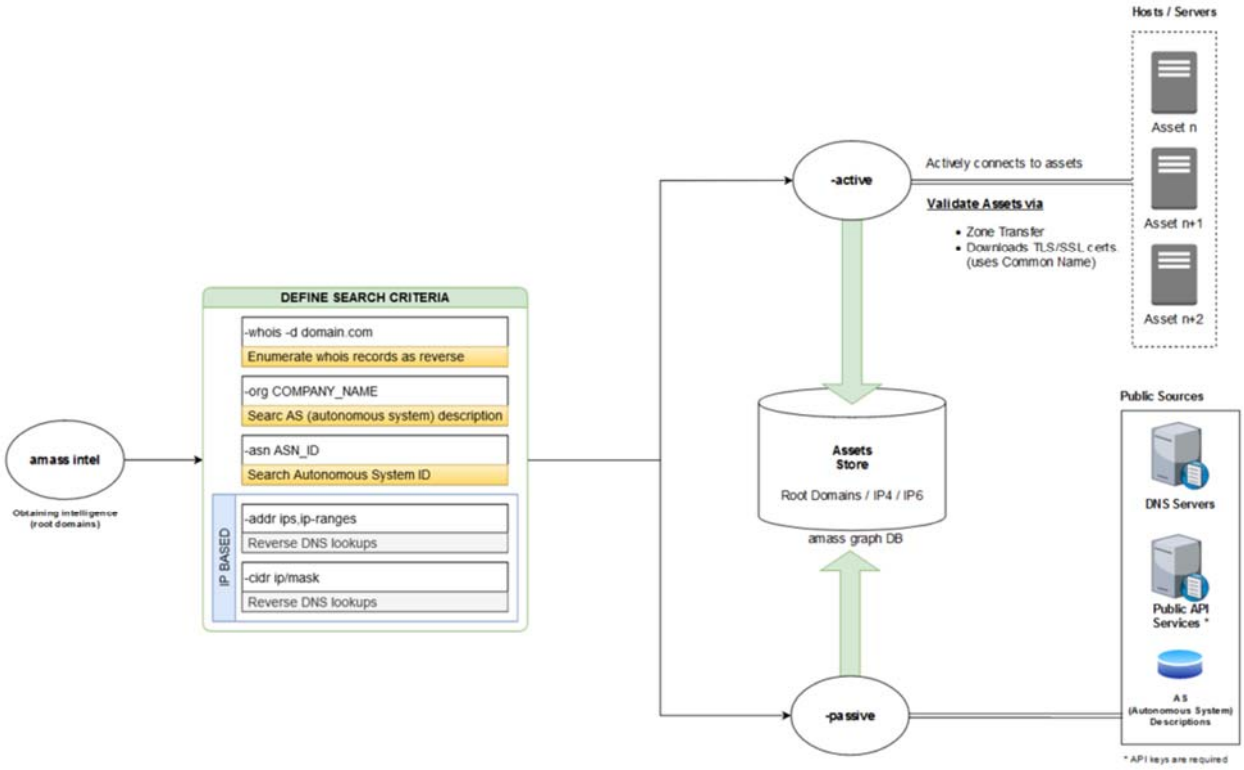
comando de inteligencia

El subcomando/módulo Amass Intel puede ayudar a recopilar inteligencia de código abierto sobre la empresa y le permite encontrar más nombres de dominio raíz asociados con la empresa. Para ver las opciones disponibles para este subcomando, simplemente escríbalo en la terminal:

```
$ acumular información
[...]
Uso: acumular información [opciones] [-whois -d DOMINIO] [-addr ADDR -asn ASN
-cidr CIDR]
-activo
Intento de captura de nombre de certificado
-valor de dirección
IPs y rangos (192.168.1.1-254) separados por comas
-asn valor
ASN separados por comas (se pueden usar varias veces)
-valor cidr
CIDR separados por comas (se pueden usar varias veces)
cadena -org
Cadena de búsqueda proporcionada contra la información de descripción de AS
-quien es
Todos los dominios proporcionados se ejecutan a través de whois inverso
```

```
[...]
```

En este punto, vale la pena señalar que otra gran ventaja de Amass es que todos los subcomandos intentan mantener la consistencia de los argumentos. En los siguientes párrafos se incluyen los parámetros de los subcomandos, se puede ver que la mayoría de ellos se usan en común. El siguiente diagrama muestra básicamente la lógica de trabajo de amasar información.



De forma predeterminada, este subcomando utilizará un conjunto de técnicas de recopilación de información y fuentes de datos, como WHOIS e IPv4Info, para obtener inteligencia organizacional y dominios principales, a menos que se deshabilite explícitamente en el archivo de configuración de Amass. Un archivo de configuración de muestra de Amass está disponible en el [repositorio de GitHub .]

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

También puede confirmar algunos de los resultados anteriores explorando manualmente las fuentes de datos. En la siguiente captura de pantalla, hicimos una búsqueda inversa de Whois para "OWASP Foundation" y le preguntamos a ViewDNS (también parte de las fuentes de datos de Amass) por dominios similares:

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

Al buscar con Amass Intel, siempre puede ejecutarlo con más opciones de configuración, por ejemplo, puede probar la transferencia de zona con el argumento --active y hacer que se conecte al servidor correspondiente para obtener los certificados SSL/TLS para extraer la información. Solo asegúrese de estar autorizado para realizar búsquedas activas contra el objetivo antes de hacerlo.

En este punto, vale la pena señalar que algunos indicadores de configuración no funcionarán con otros, en cuyo caso Amass los ignorará.

Los hallazgos de Amass pueden no ser siempre precisos por una variedad de razones, por ejemplo, las fuentes de datos utilizadas por Amass pueden no ser consistentes o estar actualizadas. Amass intenta validar aún más la información mediante consultas de DNS. Si bien Amass hace un buen trabajo, los usuarios aún deberían ejecutar más controles de validación en los resultados que no parecen relevantes para el objetivo. Esto se puede lograr usando una variedad de métodos tales como:

- Utilice utilidades (p. ej., dig, nslookup) para resolver dominios.
- Realice búsquedas de WHOIS para verificar los detalles institucionales.
- Utilice los resultados de búsqueda como dominios principales en los motores de búsqueda.

```
amass intel -org TURQUÍA
```

Devuelve los ID de ASN relacionados con la palabra Turquía. Este tipo de búsquedas de cadenas a menudo no arroja suficientes resultados. También puede agregar el modificador -active si desea que la búsqueda se realice también con métodos activos. El comando anterior buscará Turquía en las descripciones de ASN y devolverá los ASN asociados.

La clave de organización busca los ID de ASN (sistema autónomo) asociados con la expresión dada. La cadena especificada con el parámetro -org se busca en registros AS y se encuentra su ID de ASN. ASN ID es el número de sistema autónomo asignado por la Autoridad de Números Asignados de Internet (IANA), está representado por un número de identificación único en todo

el mundo de 16 dígitos. Un AS (Sistema Autónomo) se refiere a una gran red o grupo de redes con una sola política de enrutamiento (rfc1930). Los identifica en el ASN ID. Por ejemplo, el número ASN de la red de TTNET es 9121, 13335 de CloudFlare, 8517 de ULAKNET y 16509 de Amazon. Los enrutadores grandes aprovechan estos números ASN cuando es necesario realizar el enrutamiento entre redes.

Ahora intentemos encontrar los nombres de dominio en un ASN que encontramos. Echa un vistazo al comando a continuación.

```
amasar intel -active -src -ip -asn 8517 -p 80,443
```

Realizará un descubrimiento mediante técnicas activas (-active) en los puertos 80 y 443 de dominios en la red autónoma (ULAKNET) con número de ASN 8517. Utilizará certificados TLS/SSL para el descubrimiento activo. amass extraerá el certificado SSL que se conectará a todas las direcciones IP del ASN especificado y enumerará el dominio al que está asociado el certificado SSL. También mostrará las fuentes (-src) y las direcciones IP (-ip) de los dominios que encuentre.

```
amasar inteligencia -activa -ip -src -cidr 193.140.28.0/24 -p 80,443
```

Un rango de cadenas se declara con el parámetro -cidr. El número 24 representa la máscara de red y corresponde a 255.255.255.0. amass buscará y descubrirá diferentes fuentes de direcciones IP entre 193.140.28.1 y 193.140.28.254, detectando y enumerando los nombres de dominio dirigidos a estas IP. Además, el descubrimiento activo se realizará mediante certificados TLS/SSL para los puertos 80 y 443. Se conectará a cada dirección IP y obtendrá certificados SSL y enumerará los nombres de dominio mencionados en el certificado.

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

Escaneará computadoras en la red 74.6.0.6/16 usando técnicas activas. Enumerará la dirección IP y la fuente de los dominios encontrados. Realizará una consulta DNS inversa en computadoras en el rango 74.6.231.20-21.

```
amasar información -whois -d yahoo.com
```

Intenta encontrar nombres de dominio mediante la búsqueda inversa de los registros de WHOIS del dominio dado (-d) o la lista de dominios (-df). En este ejemplo, amass accede a los registros de WHOIS de yahoo.com e intenta encontrar los dominios raíz de otras organizaciones que pueden ser los mismos que esos registros de WHOIS. Es útil para encontrar otros dominios pertenecientes a una organización/empresa, pero es posible que los registros de WHOIS no siempre contengan información precisa o se mantengan confidenciales.

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

Este comando busca otros dominios con los mismos registros WHOIS en la red autónoma ULAKNET con ASN ID 8517.

A continuación se muestra una tabla que muestra las opciones y las áreas de uso del comando Intel.

ELECCIÓN	EXPLICACIÓN	MUESTRA
-ACTIVO	Utiliza métodos activos. La zona intenta la transferencia, se conecta al servidor de destino para obtener certificados SSL/TLS.	amasar intel -active -addr 192.168.2.1-64 -p 80,443,8080
-DIRECCIÓN	Especifica rangos de IP. Los rangos están separados por comas.	192.168.2.1-64,192.168.3.10-254
-ASN	Informa el ID de ASN. ASN ID es un número único asignado a grandes redes informáticas por IANNA.	acumular inteligencia -asn 13374,14618
-CIDR	Define una red. El número después de la barra inclinada define la máscara de red.	acumular inteligencia -cidr 104.154.0.0/15
-CONFIG	Especifica la ubicación del archivo de configuración de exploración.	amasar intel -config config.ini
-D	Nombres de campo separados por comas.	amasar intel -whois -d ejemplo.com
-DF	Alimenta los dominios raíz desde un archivo.	amasar intel -whois -df dominios.txt
ES	Especifica la ruta al directorio que contiene la base de datos donde se almacenarán los resultados del análisis.	Amasar Intel -dir RUTA -cidr 104.154.0.0/15
-EF	La ruta al archivo con una lista de fuentes de datos que no se utilizarán durante la investigación.	amasar intel -whois -ef excluir.txt -d ejemplo.com
-EXCLUIR	Lista de fuentes de datos que no se utilizarán en el escaneo. Se especifica separándolo con una coma.	amasar intel -whois -exclude crtsh -d ejemplo.com
-SI	Ruta al archivo con una lista de fuentes de datos para usar para escanear.	amasar intel -whois -if include.txt -d ejemplo.com
-INCLUIR	Lista de orígenes de datos que se utilizarán para escanear. Se escribe separado por comas.	amasar intel -whois -include crtsh -d ejemplo.com
-SOGA	También muestra las direcciones IP de los dominios descubiertos.	amasar intel -ip -whois -d ejemplo.com
-IPV4	También muestra las direcciones IPv4 de los dominios descubiertos.	amasar intel -ipv4 -whois -d ejemplo.com
-IPV6	También muestra las direcciones IPv6 de los dominios descubiertos.	amasar intel -ipv6 -whois -d ejemplo.com
-LISTA	Enumera los orígenes de datos que se utilizarán en el descubrimiento.	acumular información de inteligencia - lista
-INICIAR SESIÓN	Informa la ruta al archivo de registro donde se registrarán los errores.	amass intel -log amass.log -whois -d ejemplo.com

-MAX-DNS-CONSULTAS	Número máximo de consultas DNS simultáneas.	acumular intel -max-dns-consultas 200 -whois -d ejemplo.com
-ÉL	La ruta al archivo donde se guardará la salida.	amass intel -o out.txt -whois -d ejemplo.com
-ORGANO	Expresión de cadena para buscar en la instrucción AS.	amasar intel -org Facebook
-PAGS	Números de puerto separados por comas.	acumular inteligencia -cidr 104.154.0.0/15 -p 443,8080
-R	Declara los servidores DNS que se utilizarán durante el descubrimiento.	amasar intel -r 8.8.8.8,1.1.1.1 -whois -d ejemplo.com
-RF	Indica la ruta del archivo que contiene la lista de servidores DNS que se utilizarán durante el descubrimiento.	acumular información de inteligencia -rf data/resolvers.txt -whois -d ejemplo.com
-ORIGEN	Indica la fuente de donde se obtuvieron los campos descubiertos.	amasar intel -src -whois -d ejemplo.com
-SE ACABÓ EL TIEMPO	Período de tiempo de espera a considerar durante el descubrimiento.	amasar intel -timeout 30 -d ejemplo.com
-QUIEN ES	La información de WHOIS busca otros dominios similares.	amasar intel -whois -d ejemplo.com

Comando amasar enumeración

Amass enum se puede ejecutar en modo pasivo o activo. El modo pasivo es mucho más rápido, pero Amass no validará la información de DNS mediante la resolución de subdominios. Puede ejecutarlo de forma pasiva con el indicador "-passive" y no puede habilitar muchas técnicas o configuraciones, como la resolución y validación de DNS. A veces es necesario elegir el modo pasivo en lugar del modo activo, por ejemplo:

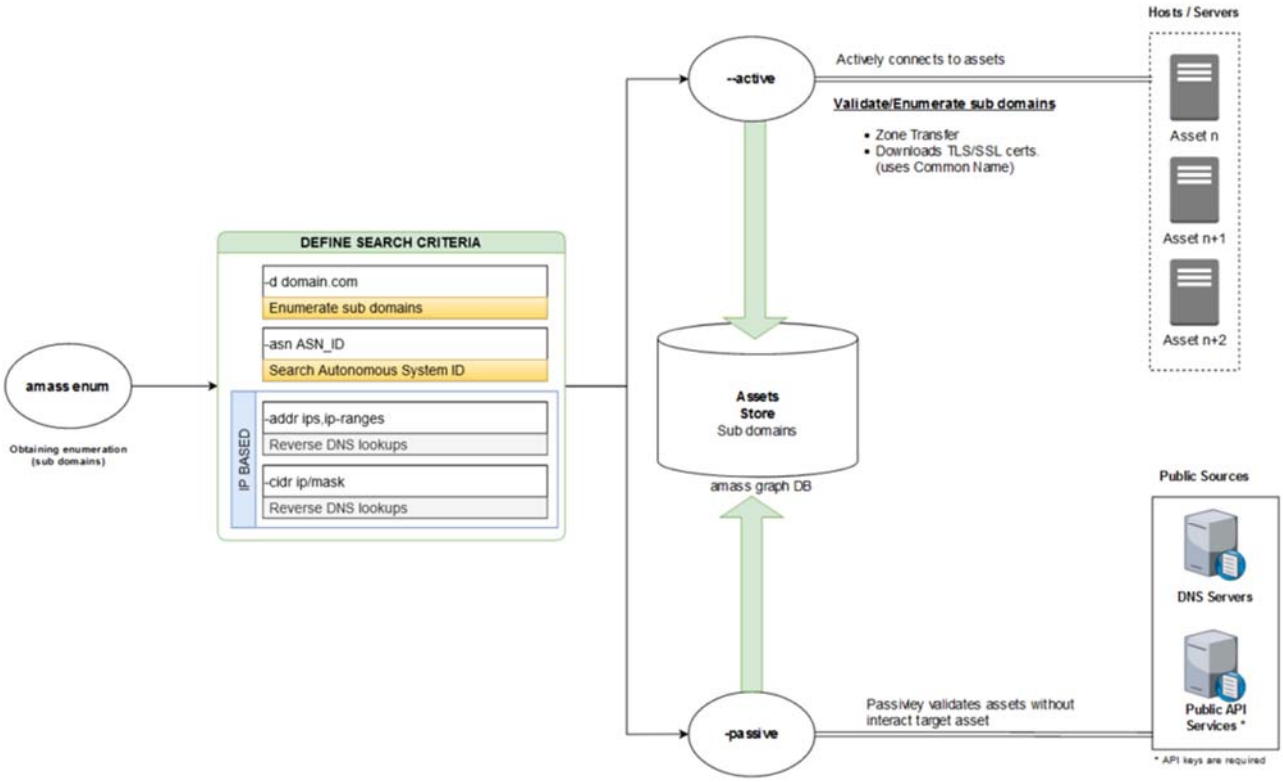
- Debido a que necesita monitorear constantemente el ámbito de destino en busca de cambios, o porque está trabajando en una interacción de phishing y buscando subdominios, necesita conocer todos los subdominios posibles que se han usado y pueden reutilizarse en el futuro.
- Es posible que deba verificar la información de DNS en una etapa posterior y poner en cola los resultados rápidamente.
- Debido a las limitaciones o los requisitos de un compromiso de seguridad, es posible que solo necesite realizar una recopilación pasiva de información.

Para ver las opciones disponibles para este subcomando, simplemente escríbalo en la terminal:

```
Uso: amass enum [opciones] -d DOMINIO

-activo
Intentar transferencias de zona y capturas de nombres de certificados
-valor de dirección
IPs y rangos (192.168.1.1-254) separados por comas
-d valor
Nombres de dominio separados por comas (se pueden usar varias veces)
-valor cidr
```

```
CIDR separados por comas (se pueden usar varias veces)
-asn valor
ASN separados por comas (se pueden usar varias veces)
```



En el siguiente ejemplo, buscamos pasivamente subdominios en Owasp.org y le pedimos a Amass que muestre las fuentes de datos donde encuentra cada subdominio:

```
$ amass enum -passive -dowasp.org -src
[...]
[ ThreatCrowd] actualización- wiki.owasp.org
[...]
BufferOver] my.owasp.org
[ crtsh ] www.lists.owasp.org
[ crtsh ] www.ocms.owasp.org
[...]
Consultando VirusTotal para subdominios owasp.org
Consultando a Yahoo por subdominios de owasp.org
[...]
```

Este subcomando llevará a cabo el descubrimiento de DNS y el mapeo de redes durante el sondeo. Vale la pena señalar en este punto que Amass enum identificará todos los subdominios, aunque el comando Amass intel ayuda a recopilar rangos de IP, ASN y dominios principales propiedad de una organización.

El uso de Amass en el modo de configuración activo significa que tendrá resultados más precisos y se podrán descubrir más activos porque puede habilitar todas las técnicas de descubrimiento de DNS. Con el "modo de configuración habilitado", buscará subdominios de dominios de certificados (por ejemplo: nombre común) realizando transferencias de zona y escaneos de puertos de servicios SSL/TLS .

generalmente se puede considerar activo, ya que realiza fuerza bruta de subdominio de varias maneras (lista de palabras, máscaras, etc.) con el indicador "-activo" habilitado . Todos los hallazgos serán validados por Amass utilizando los analizadores predeterminados o especificados:

Todas las configuraciones a continuación están relacionadas con este subcomando. Los siguientes indicadores están disponibles para la configuración:

Elección	***Explicación***	***Muestra***
-activo	Utiliza métodos activos. La zona intenta la transferencia, se conecta al servidor de destino para obtener certificados SSL/TLS.	amass enum -active -d ejemplo.com -p 80,443,8080
-ay	Indica la ruta del archivo de palabras alternativas para generar alternativas de subdominio.	amass enumeración -aw PATH -d ejemplo.com
-licenciado en Derecho	Informa una lista negra de subdominios que no se descubrirán.	amass enum -bl blah.ejemplo.com -d ejemplo.com
-blf	Especifica la ruta del archivo con la lista de subdominios en la lista negra.	amass enum -blf data/blacklist.txt -d ejemplo.com
-bruto	Utiliza la fuerza bruta en la exploración de subdominios.	amass enum -brute -d ejemplo.com
-config	Especifica la ruta al archivo de configuración INI.	amasar enumeración -config config.ini
-D	Nombres de campo separados por comas.	amass enum -d ejemplo.com
-df	Alimenta los dominios raíz desde un archivo.	amasar enumeración -df dominios.txt
es	Especifica la ruta al directorio que contiene la base de datos donde se almacenarán los resultados del análisis.	amass enum -dir PATH -d ejemplo.com
-ef	La ruta al archivo con una lista de fuentes de datos que no se utilizarán durante la investigación.	amass enumeración -ef excluir.txt -d ejemplo.com
-excluir	Lista de fuentes de datos que no se utilizarán en el escaneo. Se especifica separándolo con una coma.	amass enumeración -ef excluir.txt -d ejemplo.com
-si	Ruta al archivo con una lista de fuentes de datos para usar para escanear.	amass enumeración -ef excluir.txt -d ejemplo.com
-incluir	Lista de orígenes de datos que se utilizarán para escanear. Se escribe separado por comas.	amass enum -include crtsh -d ejemplo.com
-soga	También muestra las direcciones IP de los dominios descubiertos.	amass enumeración -ip -d ejemplo.com
-ipv4	También muestra las direcciones IPv4 de los dominios descubiertos.	amass enumeración -ip -d ejemplo.com
-ipv6	También muestra las direcciones IPv6 de los dominios descubiertos.	amass enumeración -ip -d ejemplo.com
-json	Define la ruta del archivo de salida que se guardará en formato JSON.	amass enum -json out.json -d ejemplo.com

-lista	Enumera los orígenes de datos que se utilizarán en el descubrimiento.	amasar enumeración -lista
-Iniciar sesión	Informa la ruta al archivo de registro donde se registrarán los errores.	amass enumeración -log amass.log -d ejemplo.com
-max-dns-consultas	Número máximo de consultas DNS simultáneas.	amass enumeración -max-dns-consultas 200 -d ejemplo.com
-dns-qps	Número máximo de consultas DNS por segundo en todos los solucionadores de dominio (servidor DNS).	amass enumeración -dns-qps 200 -d ejemplo.com
-rqps	Número máximo de consultas de DNS por segundo para cada resolución que no sea de confianza.	amass enumeración -dns-qps 200 -d ejemplo.com
-trqps	Número máximo de consultas de DNS por segundo para cada resolución de confianza	amass enumeración -trqps 20 -d ejemplo.com
-min-para-recursivo	Etiquetas de subdominio vistas antes de fuerza bruta recursiva (Predeterminado: 1)	amass enum -brute -min-for-recursive 3 -d ejemplo.com
-máxima profundidad	Número máximo de etiquetas de subdominio para fuerza bruta	amass enum -brute -max-depth 3 -d ejemplo.com
-nf	Ruta a un archivo que proporciona subdominios ya conocidos (de otras herramientas/fuentes)	amass enumeración -nf nombres.txt -d ejemplo.com
-noalts	Deshabilita la generación de subdominios alternativos.	amass enum -noalts -d ejemplo.com
-no recursivo	Desactiva la fuerza bruta recursiva.	amass enum -brute -norecursive -d ejemplo.com
-Él	Especifica la ruta al archivo de salida de texto.	amass enumeración -o out.txt -d ejemplo.com
-oA	Prefijo de ruta utilizado para nombrar todos los archivos de salida.	amass enumeración -oA amass_scan -d ejemplo.com
-pasivo	Realiza una ejecución completamente pasiva.	amass enumeración --passive -d ejemplo.com
-pags	Números de puerto separados por comas.	amasar enumeración -d ejemplo.com -p 443,8080
-r	Declara los servidores DNS que se utilizarán durante el descubrimiento.	amasar enumeración -d ejemplo.com -p 443,8080
-es	Direcciones IP de resolutores de DNS confiables (se pueden usar varias veces)	amass enumeración -en 8.8.8.8,1.1.1.1 -d ejemplo.com
-rf	Indica la ruta del archivo que contiene la lista de servidores DNS que se utilizarán durante el descubrimiento.	amass enumeración -en 8.8.8.8,1.1.1.1 -d ejemplo.com
-trf	Especifica la ruta a un archivo que proporciona resoluciones de DNS confiables.	amass enum -trf data/trusted.txt -d ejemplo.com
-origen	Indica la fuente de donde se obtuvieron los campos descubiertos.	amass enumeración -src -d ejemplo.com
-se acabó el tiempo	Período de tiempo de espera a considerar durante el descubrimiento.	amass enumeración -tiempo de espera 30 -d ejemplo.com

-w	Informa la ruta de un archivo de lista de palabras diferente.	amass enum -brute -w listapalabras.txt -d ejemplo.com

El uso más común del comando enum es el siguiente. Después de dar este comando, amass comienza a buscar los subdominios del nombre de dominio meb.gov.tr en Internet. Pregunta todas las fuentes de datos que puede y devuelve una pila de subdominios.

```
amass enumeración -d meb.gov.tr
amasar enumeración -pasivo -d yahoo.com -config ./passive-config.ini
```

En este escaneo, se realiza un escaneo (-pasivo) sin resolución de DNS. Suponiendo que pasiva-config.ini contiene una lista de recursos de información pasivos y claves API. La opción -passive devuelve más rápido pero menos resultados que -active.

Al usar el parámetro -v, puede aumentar el nivel de detalle del archivo amass.log y comprender mejor las características de amass mientras lo aplica. Le permite detectar fuentes de datos que no funcionan correctamente, ver servicios que bloquean su dirección IP y resoluciones de DNS que no funcionan correctamente.

amasar comando de pista

Para monitorear la superficie de ataque de un objetivo, muestra las diferencias entre el reconocimiento de los mismos objetivos. Este subcomando solo aprovecha 'output_directory' y la configuración de la base de datos remota especificada en el archivo de configuración.

Para ver las opciones disponibles para este subcomando, simplemente escríbalo en la terminal:

```
Uso: amasar pista [opciones] -d dominio
-d valor
Nombres de dominio separados por comas (se pueden usar varias veces)
-historia
Mostrar la diferencia entre todos los pares de enumeración
-último int
El número de enumeraciones recientes para incluir en el seguimiento
```

Elección	***Explicación***	***Muestra***
-config	Especifica la ruta al archivo de configuración INI.	acumular pista -config config.ini
-D	Nombres de campo separados por comas.	amass track -d ejemplo.com
-df	Alimenta los dominios raíz desde un archivo.	acumular pista -df dominios.txt
es	Especifica la ruta al directorio que contiene la base de datos donde se almacenan los resultados del análisis.	acumular pista -df dominios.txt
-historia	Muestra las diferencias entre los descubrimientos.	acumular pista -historia
-ultimo	El número de descubrimientos recientes que se incluirán en el seguimiento.	acumular pista -últimos 2

-ya que	Excluir todas las enumeraciones antes de la fecha especificada (formato: 01/02 15:04:05 2006 MST)	amasar pista -desde FECHA

```
amasar pista -d yahoo.com -últimos 2
```

El comando anterior compara los dos últimos escaneos del dominio yahoo.com.

amasar comando viz

Crea gráficos de redes visuales utilizando la información recopilada. Esta visualización es particularmente útil para interpretar las relaciones entre entidades en escaneos grandes que devuelven resultados completos. Este subcomando solo se aprovecha de la configuración de la base de datos de gráficos remotos y 'output_directory' del archivo de configuración.

Los archivos creados para la visualización se crean en el directorio de trabajo actual de forma predeterminada. Estos son los conmutadores que se pueden usar para generar resultados de DNS e infraestructura como gráficos de red:

Elección	***Explicación***	***Muestra***
-config	Especifica la ruta al archivo de configuración INI.	amasar a saber -config config.ini -d3
-D	Nombres de campo separados por comas.	amasar a saber -d3 -d ejemplo.com
-d3	Genera un archivo de simulación HTML con formato D3.js v4.	amasar a saber -d3 -d ejemplo.com
-df	Define la ruta al archivo que contiene los dominios raíz.	amasar a saber -d3 -df dominios.txt
es	Define la ruta al directorio que contiene la base de datos Graph.	amass viz -d3 -dir PATH -d ejemplo.com
-enumeración	Los resultados del escaneo identifican un descubrimiento por su número de índice de la base de datos.	amasar a saber -enum 1 -d3 -d ejemplo.com
-Él	Define la ruta al directorio donde se guardarán los archivos de salida.	amass viz -d3 -o OUTPATH -d ejemplo.com
-oA	Define un prefijo para los archivos de salida.	amasar viz -d3 -oA ejemplo -d ejemplo.com
-gexf	Formato XML de intercambio de gráficos de salida (GEXF) formateado.	amass viz -gexf -d ejemplo.com
-grafismo	Graphistry devuelve una salida con formato JSON.	amass viz -graphistry -d ejemplo.com
-maltego	Genera el archivo CSV con formato de tabla de gráficos de Maltego.	amasar a saber -maltego -d ejemplo.com

```
amasar a saber -d yahoo.com -d3 -o yahoo
```

El comando anterior muestra todos los resultados del dominio yahoo.com en un archivo con formato HTML con un gráfico asociativo. El gráfico se crea utilizando la biblioteca javascript d3 . Con la opción -o, la salida se guarda en el directorio de yahoo. El comando vizz también puede generarse en formatos Maltego, XML y JSON.

comando amasar db

Es un comando que le permite ver los datos de descubrimiento para cada escaneo realizado. Realiza la visualización y procesamiento de la base de datos. Este subcomando solo aprovecha el 'output_directory' y la configuración de la base de datos remota del archivo de configuración. Las opciones de uso para interactuar con los hallazgos de exploración en la base de datos son:

ELECCIÓN	EXPLICACIÓN	MUESTRA
-CONFIG	Especifica la ruta al archivo de configuración INI.	amasar db -config config.ini
-D	Nombres de campo separados por comas.	amass db -d ejemplo.com
-DF	Alimenta los dominios raíz desde un archivo.	amasar db -df dominios.txt
ES	Especifica la ruta al directorio de la base de datos que contiene los resultados del análisis.	amasar db -dir RUTA
-ENUMERACIÓN	Recupera información de descubrimiento a través de un número de secuencia de índice de la lista.	amasar db -enumeración 1 -mostrar
-IMPORTAR	Importa un archivo amass con formato JSON.	amasar db -importar RUTA
-SOGA	También muestra las direcciones IP de los dominios descubiertos.	amass db -show -ip -d ejemplo.com
-IPV4	También muestra las direcciones IPv4 de los dominios descubiertos.	amasar db -show -ipv4 -d ejemplo.com
-IPV6	También muestra las direcciones IPv6 de los dominios descubiertos.	amasar db -show -ipv6 -d ejemplo.com
-JSON	Define la ruta del archivo de salida que se guardará en formato JSON.	amass db -names -silent -json out.json -d ejemplo.com
-LISTA	Enumera los orígenes de datos que se utilizarán en el descubrimiento.	amasar db -lista
-NOMBRES	Trae solo dominios descubiertos.	amass db -nombres -d ejemplo.com
-SIN COLOR	Deshabilita la salida de color.	amass db -names -nocolor -d ejemplo.com
-ÉL	Especifica la ruta al archivo de salida de texto.	amass db -names -o out.txt -d ejemplo.com
-MOSTRAR	Imprime los resultados para el directorio de descubrimiento + dominios resultantes.	amasar db -mostrar
-SILENCIOSO	Deshabilita todas las salidas durante la ejecución.	amass db -names -silent -json out.json -d ejemplo.com

-ORIGEN	Indica la fuente de donde se obtuvieron los campos descubiertos.	amass db -show -src -d ejemplo.com
-RESUMEN	Imprime solo el resumen de la tabla ASN.	amass db -summary -d ejemplo.com

Para enumerar todos los detalles de sus escaneos anteriores, simplemente ejecute amass db -show para que pueda ver los resultados actuales sin necesidad de un nuevo escaneo. Si desea ver los detalles de un dominio en particular, simplemente agregue la opción -d:

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

Si prefiere una salida agradable, limpia y simple, puede imprimir los dominios/subdominios descubiertos usando la opción -names en lugar de -show.

```
amass db -dir amass4owasp -d owasp.org -enumeración 1 -mostrar
```

Muestra los resultados del descubrimiento #1 del nombre de dominio owasp.org en la base de datos registrada en el directorio amass4owasp.

Generación de claves API

Hay muchas fuentes de datos que Amass puede usar. Di una lista de ellos al principio del artículo. Sin embargo, las fuentes de datos que se enumeran a continuación necesitan la clave 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

La mayoría de estas claves API son gratuitas, pero la mayoría solo brindan resultados limitados a menos que tenga una clave API paga. Los gratuitos son mejores que nada. Deberá encontrar el sitio web para cada uno de los servicios anteriores, luego registrarse y obtener una clave API. Esta es una tarea tediosa y que consume mucho tiempo, pero un buen descubrimiento no viene sin sacrificio. Puedes hacerlo. Una vez que tenga todas sus claves de API, péguelas en el archivo de configuración de Amass. Consulte aquí un archivo de configuración de ejemplo completo . A continuación se muestra el contenido de un archivo de configuración. A los que escriben Pagado se les paga. Obtenga cualquiera de las fuentes de datos usando la API en el archivo de muestra, agréguelas de la siguiente manera y cree su propio archivo de configuración de amasar. Luego guarde el archivo con el nombre amassconfig.ini, por ejemplo:

```
# https://passivedns.cn (Contacto)
[fuentes_de_datos.360PassiveDNS]
[ data_sources.360PassiveDNS.Credentials ]
apikey = tamañoozelapicode

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

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

Ahora, cuando use amass, especifique el archivo de configuración con el parámetro -config de la siguiente manera. Esto aumentará el número y la calidad de sus descubrimientos de inteligencia y enumeración. Le recomiendo encarecidamente que haga esto para estar un paso por delante de los demás.

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

directorio de salida

amass mantiene los archivos de registro y de salida de la última sesión de análisis en ~/.config/amass de forma predeterminada. Estos archivos se restablecen cuando se realiza un nuevo escaneo. El archivo de registro debe examinarse al final del escaneo, ya que registra cómo avanza el proceso de escaneo y los posibles errores. De manera similar, la salida del escaneo se almacena en este directorio en formato CSV. Puede ser útil usar un directorio de repositorio diferente para cada exploración. Puede dar la opción -dir al comando para esto. Mira el ejemplo a continuación:

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

Con el comando anterior, se buscará la red TURKSAT con ASN (red autónoma) número 47524 y los descubrimientos se guardarán en el directorio turksat.

Referencias

Sitio web del proyecto Amass: https://owasp-amass.com/
Código fuente de Amass: https://github.com/OWASP/Amass
Guía del usuario: https://github.com/OWASP/Amass/blob/master/doc / user_guide.md
Ejemplos de uso: https://github.com/OWASP/Amass/blob/master/doc/tutorial.md
Guía de usuario de Haklukes: https://hakluke.medium.com/haklukes-guide-to- amass- cómo-usar-amass-más-eficaz-para-recompensas-de-errores-7c37570b83f7

Derechos de autor