HackerDivulgation.com

HTTP-SUITE

Es una pequeña suite que permite escanear dominios. Cuenta con scripts para: enumerar subdominios, listar los DNS, encontrar paneles de administración, escanear puertos, etc.

Proyecto: HTTP-Suite-Github

Contenido

- Instalación
- Opciones
- Uso
 - Whois
 - Headers
 - o Crawling
 - Buscar Directorios
 - o Buscar panel de administración
 - Escanear puertos
 - Enumerar DNS
 - Escanear subdominios
- Referencias

Instalación

Clonar el repositorio del proyecto,

git clone https://github.com/whoamisec75/httpsuite

Entrar al repositorio descargado.

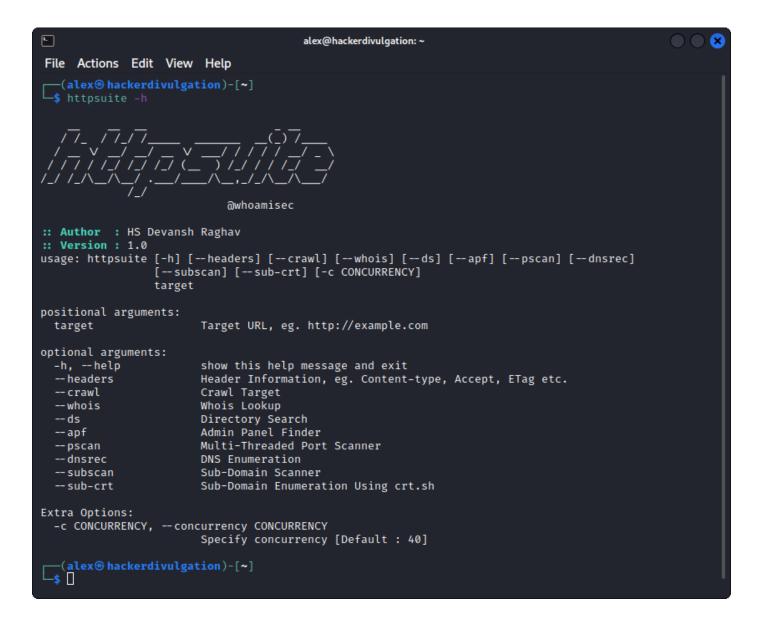
cd httpsuite/

Ejecutar el archivo de instalación.

Opciones

Para dezplegar la ayuda se usa el parámetro -h.

httpsuite -h



Argumento Opcional	Significado
headers	Información de Cabeceras. Content-type, Accept, ETag, etc.
crawl	Objetivo Crawl

Argumento Opcional	Significado
whois	Whois Lookup
ds	Busqueda de directorios
apf	Buscador de paneles de administración
pscan	Escaner de puertos multihilo
dnsrec	Enumeración DNS
subscan	Escaner de subdominios
sub-crt	Escaner de subdominios usando el script crt.sh

En la seccion de uso se explicará el uso que tiene cada argumento.

USO

¡¡ Las siguientes pruebas se realizaron escaneando el propio dominio de <u>HackerDivulgation.com</u> por lo que no se interfiere con terceros. Para realizar estas mismas pruebas se puede usar el sitio <u>VulnWeb</u> desarrollado por <u>Acutinex</u>, nunca usar en sitios sin autorización !!

Whois

Se obtendrá información del dominio como: propietario del dominio, IP del servidor, dirección, país, etc.

httpsuite http://DOMINIO.COM --whois

```
•
                                         alex@hackerdivulgation: ~
File Actions Edit View Help
  -(alex⊛hackerdivulgation)-[~]
$ https://hackerdivulgation.com --whois
                             ลwhoamisec
:: Author : HS Devansh Raghav
:: Version : 1.0
[INF] Whois Lookup :
[RES] asn_registry: arin
[RES] asn: 26496
[RES] asn_cidr: 68.178
[RES] asn_country_code: US
[RES] asn_date: 2005-04-12
[RES] query: 68.178
[RES] cidr: 68.178.
[RES] name: GO-DADDY-COM-LLC
     handle: NET-68-
[RES] range: 68.178
                           - 68.178
[RES] description: GoDaddy.com LLC
[RES] country: US
[RES] state: AZ
     city: Scottsdale
                                    Suite 2
[RES] address:
[RES] postal_code:
[RES] emails: [
[RES] created: 2005-04-12
                                                      ' ]
[RES] updated: 2014-02-25
    (alex⊕hackerdivulgation)-[~]
```

Headers

Las cabeceras HTTP se utilizan para transmitir información adicional entre el cliente y servidor, constan de una petición y una respuesta. El programa trasmitirá una cabecera, con la respuesta del servidor se obtendrá información como el servicio que se está ejecutando para http, el Keep-Alive (tiempo de espera), etc.

httpsuite http://DOMINIO.COM --headers

```
<u>-</u>
                                        alex@hackerdivulgation: ~
File Actions Edit View Help
  -(alex⊛hackerdivulgation)-[~]
$ https://hackerdivulgation.com --headers
                            @whoamisec
:: Author : HS Devansh Raghav
:: Version : 1.0
[INF] Headers ⇒
[RES] Date: Tue, 04 Jan 2022 23:38:08 GMT
[RES] Server: Apache
[RES] Upgrade: h2,h2c
[RES] Connection: Upgrade, Keep-Alive
[RES] Last-Modified: Sat, 01 Jan 2022 17:18:36 GMT
[RES] ETag: "1cc04e7-61a-5d4887a5742d4-gzip"
[RES] Accept-Ranges: bytes
[RES] Vary: Accept-Encoding
[RES] Content-Encoding: gzip
[RES] Content-Length: 763
[RES] Keep-Alive: timeout=5
[RES] Content-Type: text/html
   (alex⊛hackerdivulgation)-[~]
```

Crawling

Crawling es la técnica que usan los buscadores para indexar páginas web usando un script automátizado o bots.

httpsuite http://DOMINIO.COM --crawl

Buscar Directorios

Con esta funcionalidad se podrán buscar directorios dentro de la página web, por ejemplo: carpetas que contengan hojas de estilos, código en JS, archivos de configuración del sitio, archivos de conexión, etc.

httpsuite http://DOMINIO.COM --ds

```
<u>-</u>
                                                alex@hackerdivulgation: ~
File Actions Edit View Help
   -(alex⊛hackerdivulgation)-[~]
httpsuite http://hackerdivulgation.com --ds
:: Author : HS Devansh Raghav
:: Version : 1.0
[INF] Searching Directories ...
[RES] http://hackerdivulgation.com/
                                                        [200]
[RES] http://hackerdivulgation.com,
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/Books requests.exceptions.ConnectionError: http://hackerdivulgation.com/Business
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/Browser
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/CVS
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/CPAN
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/ChangeLog requests.exceptions.ConnectionError: http://hackerdivulgation.com/CVS/Repository
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/C
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/Computers
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/Creatives requests.exceptions.ConnectionError: http://hackerdivulgation.com/CYBERDOCS31
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/CVS/Entries
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/Contact
```

Buscar panel de administración

A diferencia de la funcionalidad anterior esta se enfoca en encontrar panales de adminitración de las páginas web. Esto se realiza con una lista de los nombres típicos de directorios de administración.

httpsuite http://DOMINIO.COM --apf

```
alex@hackerdivulgation: ~
File Actions Edit View Help
  -(alex⊛hackerdivulgation)-[~]
 -$ httpsuite http://hackerdivulgation.com --apf
                                 กิพhoamisec
:: Author : HS Devansh Raghav
:: Version : 1.0
[INF] Finding Admin Panels...
[RES] http://hackerdivulgation.com/
                                                 [200]
[RES] http://hackerdivulgation.com/
      requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin/loginsuccess.php
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin_main.html requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin/log.php
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin/main_page.php
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin/main.php/
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/administrator.php
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin_login.php] requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin/login.html
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/ADMIN/login.html
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/administrator/index.php
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin-login.asprequests.exceptions.ConnectionError: http://hackerdivulgation.com/adminLogin/
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin/login
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/administratorlogin.php
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/ADMIN/login.php
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/adminLogin.asprequests.exceptions.ConnectionError: http://hackerdivulgation.com/admin_login.html
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin/login.php
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/administrator/index.html
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/administrators/
       requests.exceptions.ConnectionError: http://hackerdivulgation.com/admin/list_gallery.php
```

Escanear puertos

Se escanean y se muestran los puertos abiertos del sitio. Se espeficica hasta que número de puerto se desea escanear. Este escaneo se puede complementar con otras herramientas como NMAP.

httpsuite http://DOMINIO.COM --pscan

Enumerar DNS

Es útil para conocer los registros de zona del dominio.

httpsuite http://DOMINIO.COM --dnsrec

```
alex@hackerdivulgation: ~
File Actions Edit View Help
(alex⊕ hackerdivulgation)-[~]
$ httpsuite http://hackerdivulgation.com --dnsrec
                                         @whoamisec
:: Author : HS Devansh Raghav
:: Version : 1.0
[INF] Starting DNS Enumeration...
         hackerdivulgation.com.
                                            10800
                                                                    A
MX
        hackerdivulgation.com. 3600
hackerdivulgation.com. 3600
hackerdivulgation.com. 3600
hackerdivulgation.com. 600
[RES]
                                                         IN
                                                                    NS
SOA
[RES]
                                                         IN
                                                                    SOA
        hackerdivulgation.com.
hackerdivulgation.com.
                                                                    NS
TXT
                                            3600
[RES] DMARC Record Not Found!
__(alex⊛hackerdivulgation)-[~]
```

Escanear subdominios

Con este escaneo se puede además verificar si se está usando un subdominio para administración o para un panel de usuarios registrados.

httpsuite http://DOMINIO.COM --subscan

```
alex@hackerdivulgation: ~
File Actions Edit View Help
  -(alex⊛hackerdivulgation)-[~]
httpsuite http://hackerdivulgation.com --subscan
                            @whoamisec
:: Author : HS Devansh Raghav
:: Version : 1.0
[INF] Scanning Subdomains ...
[RES] http://www.hackerdivulgation.com
[RES] http://test.hackerdivulgation.com
[RES] http://admin.hackerdivulgation.com
[RES] http://mail.hackerdivulgation.com
[RES] http://autoconfig.hackerdivulgation.com
[RES] http://www.admin.hackerdivulgation.com
[RES] http://autoconfig.admin.hackerdivulgation.com
   [~] (alex⊛hackerdivulgation)
```

REFERENCIAS

- 1. Proyecto publicado en Github. https://github.com/whoamisec75/httpsuite
- 2. Página para probar vulnerabilidades. http://www.vulnweb.com/



Este obra está bajo una <u>licencia de Creative Commons Reconocimiento-NoComercial-</u> SinObraDerivada 4.0 Internacional.