

MÓDULO: VULNERABILIDADES WEB COMUNES

Actividad de aprendizaje:

La siguiente actividad tiene como objetivo que el Aprendiz identifique las diferentes herramientas de fingerprinting web que existen, para lo cual cada aprendiz tendrá acceso a dos máquinas de laboratorio tipo VPS donde una de estas actuará como servidor de la aplicación de laboratorio y desde la otra se realizarán las pruebas de funcionamiento de las diferentes herramientas.

Tipo de Ejercicio: individual - revisión en grupo

Para esta actividad el aprendiz deberá:

Investigar sobre las herramientas de fingerprinting web disponibles, realizar la instalación de las mismas en la máquina de ataque y realizar una prueba de funcionamiento de cada una.

Ejemplo de alguna de estas herramientas:

- WhatWeb
- BlindElephant
- Wig

WhatWeb

WhatWeb identifica sitios web. Su objetivo es responder a la pregunta "¿Qué es ese sitio web?". WhatWeb reconoce tecnologías web como sistemas de gestión de contenidos (CMS), plataformas de blogs, paquetes de estadísticas/análisis, bibliotecas JavaScript, servidores web y dispositivos integrados.

WhatWeb cuenta con más de 1.800 plugins, cada uno de los cuales reconoce algo diferente. WhatWeb también identifica números de versión, direcciones de correo electrónico, ID de cuentas, módulos de marcos web, errores SQL y mucho más.

WhatWeb puede ser sigiloso y rápido, o minucioso pero lento. WhatWeb admite un nivel de agresión para controlar el equilibrio entre velocidad y fiabilidad. Cuando visita un sitio web en su navegador, la transacción incluye muchos indicios de qué tecnologías web están impulsando ese sitio web. A veces, una sola visita a una página web contiene información suficiente para identificar un sitio web, pero cuando no es así, WhatWeb puede interrogar al sitio web más a fondo. El nivel de agresión predeterminado, denominado "sigiloso", es el más rápido y sólo requiere una solicitud HTTP de un sitio web. Es adecuado para escanear sitios web públicos. Se desarrollaron modos más agresivos para su uso en pruebas de penetración.

```
(kali㉿kali)-[~]  
$ whatweb
```

[illegible]

WhatWeb - Next generation web scanner version 0.5.5.
Developed by Andrew Horton (urbanadventurer) and Brendan Coles (bcoles)
Homepage: <https://www.morningstarsecurity.com/research/whatweb>

```
Usage: whatweb [options] <URLs>
```

```
<TARGETS>                Enter URLs, hostnames, IP addresses, filenames or
                           IP ranges in CIDR, x.x.x-x, or x.x.x.x-x.x.x.x
                           format.
--input-file=FILE, -i      Read targets from a file.

--aggression, -a=LEVEL     Set the aggression level. Default: 1.
1. Stealthy                Makes one HTTP request per target and also
                           follows redirects.
3. Aggressive               If a level 1 plugin is matched, additional
                           requests will be made.

--list-plugins, -l          List all plugins.
--info-plugins, -I=[SEARCH] List all plugins with detailed information.
                           Optionally search with a keyword.

--verbose, -v               Verbose output includes plugin descriptions.
```

Inicializamos whatweb en Kali y vemos las opciones que nos proporciona.

Ur1

```
--input-file=FILE, -i
--aggression, -a=LEVEL
1. Stealthy
3. Aggressive
--list-plugins, -l
--info-plugins, -I=[Search]
--verbose, -v
```

Uso.

Iniciamos nuestra Kali junto con la máquina a atacar en este caso metasploitable2.

Conseguimos la ip de la meta y lo analizamos con whatweb.

```
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ clera  
-bash: clera: command not found  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:63:aa:19  
          inet addr:192.168.1.26  Bcast:192.168.1.255  Mask:255.255  
          inet6 addr: fe80::a00:27ff:fe63:aa19/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:195 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:15022 (14.6 KB)  TX bytes:12902 (12.5 KB)  
          Base address:0xd020  Memory:f0200000-f0220000
```

```
kali@kali: ~  
(kali@kali)-[~]  
$ whatweb 192.168.1.26 -a 3 --verbose  
WhatWeb report for http://192.168.1.26  
Status      : 200 OK  
Title       : Metasploitable2 - Linux  
IP          : 192.168.1.26  
Country     : RESERVED, ZZ  
  
Summary     : Apache[2.2.8], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2  
], PHP[5.5.2.4-2ubuntu5.10], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]  
  
Detected Plugins:  
[ Apache ]  
    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 NT. 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.  
  
    Version      : 2.2.8 (from HTTP Server Header)  
    Google Dorks : (3)  
    Website      : http://httpd.apache.org/  
  
[ HTTPServer ]  
    HTTP server header string. This plugin also attempts to  
    identify the operating system from the server header.  
  
    OS           : Ubuntu Linux  
    String       : Apache/2.2.8 (Ubuntu) DAV/2 (from server string)  
  
[ PHP ]  
    PHP is a widely-used general-purpose scripting language  
    that is especially suited for Web development and can be  
    embedded into HTML. This plugin identifies PHP errors,  
    modules and versions and extracts the local file path and  
    username if present.
```

En esta ocasión he puesto el parámetro de agresión a nivel 3 ya que es un entorno controlado y no supone ningún riesgo.

Resultados:

```
kali@kali: ~  
that is especially suited for Web development and can be  
embedded into HTML. This plugin identifies PHP errors,  
modules and versions and extracts the local file path and  
username if present.  
  
Version      : 5.2.4-2ubuntu5.10  
Version      : 5  
Google Dorks: (2)  
Website      : http://www.php.net/  
  
[ WebDAV ]  
Web-based Distributed Authoring and Versioning (WebDAV) is  
a set of methods based on the Hypertext Transfer Protocol  
(HTTP) that facilitates collaboration between users in  
editing and managing documents and files stored on World  
Wide Web servers. - More Info:  
http://en.wikipedia.org/wiki/WebDAV  
  
Version      : 2  
  
[ X-Powered-By ]  
X-Powered-By HTTP header  
  
String       : PHP/5.2.4-2ubuntu5.10 (from x-powered-by string)  
  
HTTP Headers:  
HTTP/1.1 200 OK  
Date: Thu, 01 Feb 2024 10:43:55 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Connection: close  
Transfer-Encoding: chunked  
Content-Type: text/html  
  
(kali@kali) - [~]  
$
```

Status: 200 OK

Título de la máquina/web.

Ip.

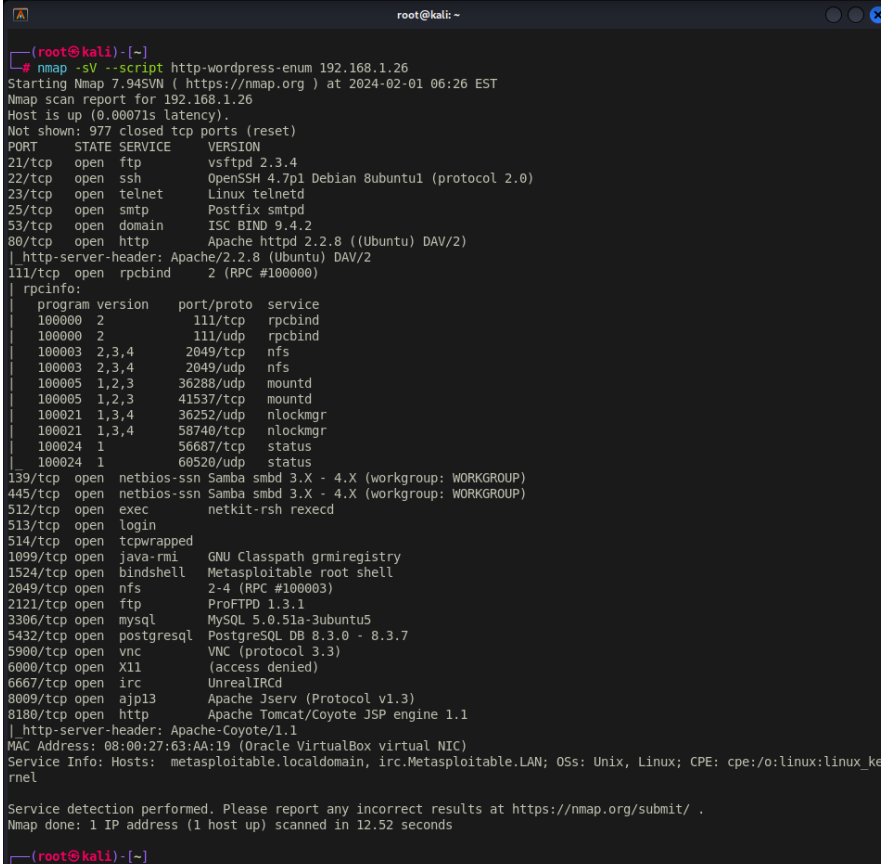
Country.

En el resumen nos muestra los plugins que utiliza y alguna información útil para saber qué son: APACHE 2.2.8, HTTPSERVER Ubuntu Linux, PHP 5,5.2.4, WEBDAV 2, X-POWERED-BY PHP 5.2.4.

BlindElephant

En este caso la aplicación utiliza una versión antigua de Python y no puedo instalarla en mi Kali ya que viene deprecated. En su lugar, utilizaré un script de NMAP para enumerar los plugins.

```
nmap -sV --script http-wordpress-enum 192.168.1.26
```



```
(root@kali)-[~]
# nmap -sV --script http-wordpress-enum 192.168.1.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-01 06:26 EST
Nmap scan report for 192.168.1.26
Host is up (0.00071s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind        2 (RPC #100000)
|_ rpcinfo:
|_  program version  port/proto  service
|_  100000  2             111/tcp    rpcbind
|_  100000  2             111/udp    rpcbind
|_  100003  2,3,4         2049/tcp   nfs
|_  100003  2,3,4         2049/udp   nfs
|_  100005  1,2,3         36288/udp  mountd
|_  100005  1,2,3         41537/tcp  mountd
|_  100021  1,3,4         36252/udp  nlockmgr
|_  100021  1,3,4         58740/tcp  nlockmgr
|_  100024  1             56687/tcp  status
|_  100024  1             60520/udp  status
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
|_ http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:63:AA:19 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.52 seconds

(root@kali)-[~]
```

Con este comando/script logramos ver que utiliza Apache 2.2.8 y una máquina Ubuntu con DAV 2.

Además utiliza Apache Jserv v1.3 y apache Tomcat/Coyote JSP engine 1.1 en los puertos 8009 y 8180 respectivamente.

Wig

Wig es una herramienta de recopilación de información sobre aplicaciones web, que puede identificar numerosos sistemas de gestión de contenidos y otras aplicaciones administrativas.

La huella digital de la aplicación se basa en sumas de comprobación y concordancia de cadenas de archivos conocidos para diferentes versiones de CMS. Como resultado, se calcula una puntuación para cada CMS detectado y sus versiones. El cálculo de la puntuación se basa en pesos y en la cantidad de "aciertos" para una suma de comprobación determinada.

Wig también intenta adivinar el sistema operativo del servidor basándose en las cabeceras 'server' y 'x-powered-by'. En Wig se incluye una base de datos que contiene valores de cabecera conocidos para diferentes sistemas operativos, lo que permite a Wig adivinar las versiones de Microsoft Windows y la distribución y versión de Linux.

```
root@kali: ~  
(root@kali)-[~]  
# wig -h  
usage: wig [-h] [-l INPUT_FILE] [-q] [-n STOP_AFTER] [-a] [-m] [-u] [-d] [-t THREADS] [--no_cache_load]  
          [--no_cache_save] [-N] [--verbosity] [--proxy PROXY] [-w OUTPUT_FILE]  
          [url]  
  
WebApp Information Gatherer  
  
positional arguments:  
  url                The url to scan e.g. http://example.com  
  
options:  
  -h, --help          show this help message and exit  
  -l INPUT_FILE        File with urls, one per line.  
  -q                  Set wig to not prompt for user input during run  
  -n STOP_AFTER        Stop after this amount of CMSs have been detected. Default: 1  
  -a                  Do not stop after the first CMS is detected  
  -m                  Try harder to find a match without making more requests  
  -u                  User-agent to use in the requests  
  -d                  Disable the search for subdomains  
  -t THREADS          Number of threads to use  
  --no_cache_load      Do not load cached responses  
  --no_cache_save      Do not save the cache for later use  
  -N                  Shortcut for --no_cache_load and --no_cache_save  
  --verbosity, -v      Increase verbosity. Use multiple times for more info  
  --proxy PROXY        Tunnel through a proxy (format: localhost:8080)  
  -w OUTPUT_FILE       File to dump results into (JSON)  
  
(root@kali)-[~]  
#
```

Sus opciones son:

- h -> Para ayuda.
- l -> Fichero con URLs, una por línea.
- q -> Configure Wig para que no solicite la entrada del usuario durante la ejecución.
- n STOP_AFTER -> Parar después de que la cantidad de CMS ha sido detectada. Por defecto 1.
- a -> No parar después de haber detectado el primer CMS
- m -> Esforzarse para encontrar un match antes de hacer más peticiones.
- u -> User-agent para utilizar en las peticiones.
- d -> Desactivar la búsqueda de subdominios.

-t -> Número de threads a usar.

--no_cache_load -> No cargar peticiones cacheadas.

--no_cache_save -> No guardar el cache para uso posterior.

-N -> Shortcut de --no_cache_load y --no_cache_save.

-v -> verbosidad

--proxy -> Túnel proxy formato localhost:8080

-W -> creación de fichero para volcar los datos obtenidos en formato JSON.

Utilización.

```
root@kali: ~  
--proxy PROXY    Tunnel through a proxy (format: localhost:8080)  
-w OUTPUT_FILE  File to dump results into (JSON)  
  
(root@kali)-[~]  
# wig 192.168.1.26 -a -m -d -N -vvv -w /home/kali/Desktop/wig_test.JSON  
  
wig - WebApp Information Gatherer  
  
http://192.168.1.26 does not redirect  
Scanning http://192.168.1.26...  
Getting title ...  
- Found title: Metasploitable2 - Linux  
Error page detection ...  
- Error page fingerprint: f242c77ee68efb97a52294993af67426, 8912b88d534a9772181390a342d6debb - /  
Determining CMS type ...  
Checking fingerprint group no. 0 ...  
Checking fingerprint group no. 1 ...  
Checking fingerprint group no. 2 ...  
Checking fingerprint group no. 3 ...  
Checking fingerprint group no. 4 ...  
Checking fingerprint group no. 5 ...  
Checking fingerprint group no. 6 ...  
Checking fingerprint group no. 7 ...  
Checking fingerprint group no. 8 ...  
Checking fingerprint group no. 9 ...  
Checking fingerprint group no. 10 ...  
Checking fingerprint group no. 11 ...  
Checking fingerprint group no. 12 ...  
Checking fingerprint group no. 13 ...  
Checking fingerprint group no. 14 ...  
Checking fingerprint group no. 15 ...  
Checking fingerprint group no. 16 ...  
Checking fingerprint group no. 17 ...  
Checking fingerprint group no. 18 ...  
Checking fingerprint group no. 19 ...  
Checking fingerprint group no. 20 ...  
Checking fingerprint group no. 21 ...  
Checking fingerprint group no. 22 ...  
Checking fingerprint group no. 23 ...  
Checking fingerprint group no. 24 ...  
Detecting platform ...  
- Found platform PHP 5.2.4-2ubuntu5.10  
- Found platform Apache 2.0.61  
- Found platform Apache 2.0.62  
- Found platform Apache 2.0.63  
- Found platform Apache 2.0.64  
- Found platform Apache 2.0.65  
- Found platform Apache 2.2.10  
- Found platform Apache 2.2.6  
- Found platform Apache 2.2.7  
- Found platform Apache 2.2.8  
- Found platform Apache 2.2.9
```

```
~/Desktop/wig_test.JSON.json [Read Only] - Mousepad
File Edit Search View Document Help
1 [
2 {
3   "data": [
4     {
5       "category": "CMS",
6       "name": "phpMyAdmin",
7       "version": "5.2.4"
8     },
9     {
10      "category": "Platform",
11      "name": "Apache",
12      "version": "2.2.8"
13    },
14    {
15      "category": "Platform",
16      "name": "PHP",
17      "version": "5.2.4-2ubuntu5.10"
18    },
19    {
20      "category": "Platform",
21      "name": "dav",
22      "version": "2"
23    },
24    {
25      "category": "OS",
26      "name": "Ubuntu",
27      "version": "8.04"
28    },
29    {
30      "category": "Interesting",
31      "note": "Test directory",
32      "url": "/test/"
33    },
34    {
35      "category": "Interesting",
36      "note": "PHP info file",
37      "url": "/phpinfo.php"
38    },
39    {
40      "category": "Interesting",
41      "note": "Directory Listing",
42      "url": "/test/"
43    },
44    {
45      "category": "Interesting",
46      "note": "phpMyAdmin readme",
47      "url": "/readme"
48    }
49  ]
50 }
```

```
wig 192.168.1.26 -a -m -d -N -vvv -w
/home/kali/Desktop/wig_test.JSON
```

Descripción del comando.

Url -> 192.168.1.26

-a -> para seguir después de encontrar el primer CMS.

-m -> Para esforzarse más antes de hacer más peticiones.

-d -> Desactivar la búsqueda de subdominios.

-N -> Shortcut.

-vvv -> Mayor verbosidad.

-w -> dirección en la que quiero que guarde el fichero en formato JSON.