Reconocimiento de Pentesting en BeeBox

En esta tarea de laboratorio se requiere realizar el reconocimiento de una máquina virtual dada con objetivo de encontrar vulnerabilidades de cualquier tipo en la información que esta expone a la web.

Escaneo de puertos

La primera etapa que se va a llevar a cabo va a ser un escaneo de puertos con ***nmap***, para comprobar que tipo de servicios está publicando la máquina, para ello se rastrea la máquina objetivo haciendo uso de ***nmap -sn 192.168.1.0/24****, analizando así todos los dispositivos que haya en el bloque de direcciones de la red*:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 15:42 EST
Nmap scan report for 192.168.1.10
Host is up (0.00018s latency).
MAC Address: D0:39:57:0E:2F:7B (Liteon Technology)
Nmap scan report for 192.168.1.52
Host is up (0.00061s latency).
MAC Address: 08:00:27:66:0C:CB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.11
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 27.93 seconds
```

Se puede verificar que, a parte de la máquina Kali, hay dos equipos más, siendo que uno de ellos parecer ser únicamente una emulación de una NIC de *virtualbox*, por lo que se procederá a analizar la otra ip, esto también puede hacerse con nmap, y es que se van a comprobar los servicios que está publicando esta IP en sus puertos abiertos por medio de ***nmap -sV 192.168.1.52***:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.52
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 16:22 EST
Nmap scan report for 192.168.1.52
Host is up (0.00026s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patc
h mod_ssl/2.2.8 OpenSSL/0.9.8g)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp  open  ssl/http    Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patc
h mod_ssl/2.2.8 OpenSSL/0.9.8g)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
666/tcp  open  doom?
3306/tcp open  mysql       MySQL 5.0.96-0ubuntu3
5901/tcp open  vnc         VNC (protocol 3.8)
6001/tcp open  X11         (access denied)
8080/tcp open  http        nginx 1.4.0
8443/tcp open  ssl/http    nginx 1.4.0
9080/tcp open  http        lighttpd 1.4.19
```

Gracias a este primer escaneo se puede comprobar que, además de la aplicación web, el servicio dispone de conexión remota por ssh, así como un servicio de consola sobre http que utiliza una versión inferior de OpenSSH a la que se usa en el puerto 22, también se observa que las versiones tanto de apache como de nginx están desactualizadas.

Escaneo de vulnerabilidades

Habiendo recabado un poco de información preliminar, ahora se da paso al escaneo de los servicios vulnerables, para ello se lanzará un escaneo con la herramienta ***nikto***:

```
+ mod_ssl/2.2.8 OpenSSL/0.9.8g - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow
 a remote shell.
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community
/attacks/Cross_Site_Tracing
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict
 access to allowed sources. See: OSVDB-561
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to auth
orized hosts.
+ /icons/: Directory indexing found.
+ /README: README file found.
+ /INSTALL.txt: Default file found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to
 authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:           2025-11-11 11:44:03 (GMT-5) (15 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

De entre toda la información que brinda la herramienta, la vulnerabilidad más grave es la de OpenSSL, siendo que al estar desactualizada, puede ser posible obtener una shell remota por medio de desbordamiento de buffer.

Fuerza Bruta en directorios de archivos

Una vez analizado los servicios expuestos superficialmente, es hora de explorar los archivos que el servidor tiene publicados, para ello se va a disponer de la herramienta de ***gobuster***, para realizar un escaneo de los endpoints que tiene la web de la máquina objetivo, para comprobar si hay rutas de interés a las que se pueda acceder simplemente navegando a ellas, para hacer esto el comando indicado es ***gobuster dir -u http://192.168.1.52 -w /usr/share/wordlists/dirb/common.txt***:

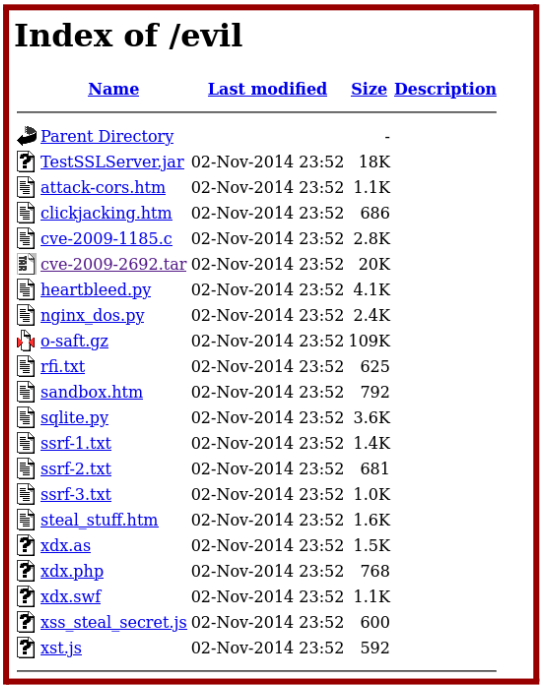
```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -u http://192.168.1.52 -w /usr/share/wordlists/dirb/common.txt
[sudo] password for kali:
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.52
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 379]
/.htaccess            (Status: 403) [Size: 379]
/.hta                 (Status: 403) [Size: 374]
/crossdomain.xml      (Status: 200) [Size: 200]
/crossdomain          (Status: 200) [Size: 200]
/drupal               (Status: 301) [Size: 403] [--> http://192.168.1.52/drupal/]
/evil                 (Status: 301) [Size: 401] [--> http://192.168.1.52/evil/]
/index.html           (Status: 200) [Size: 588]
/index                (Status: 200) [Size: 45]
/phpmyadmin           (Status: 301) [Size: 407] [--> http://192.168.1.52/phpmyadmin/]
/README               (Status: 200) [Size: 2491]
/server-status        (Status: 200) [Size: 6198]
/webdav               (Status: 301) [Size: 403] [--> http://192.168.1.52/webdav/]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

Se puede apreciar que en el análisis han aparecido varios endpoints que cuelgan de la web de la máquina objetivo, en la última etapa del análisis se cubrirán los resultados del análisis realizado a lo largo del informe.

Endpoints vulnerables dentro de la página objetivo

Se han apreciado múltiples vistas que contienen contenido listado en la página, así como de paneles de administración

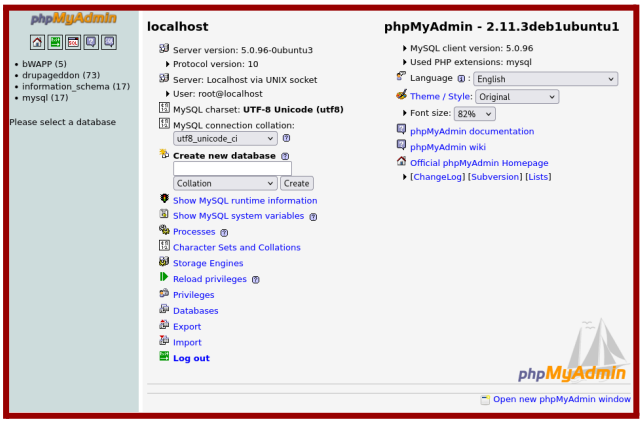
Empezando por los endpoints de contenido, se observan dos vistas ***/webdav*** y ***/evil***, la primera contiene información de bajo interés, por el contrario, al entrar al directorio "malvado", se pueden observar distintos ficheros con información acerca de como vulnerar servicios, así como varios *exploits*, escritos en C:



Index of /evil

Name	Last modified	Size	Description
Parent Directory		-	
TestSSLServer.jar	02-Nov-2014 23:52	18K	
attack-cors.htm	02-Nov-2014 23:52	1.1K	
clickjacking.htm	02-Nov-2014 23:52	686	
cve-2009-1185.c	02-Nov-2014 23:52	2.8K	
cve-2009-2692.tar	02-Nov-2014 23:52	20K	
heartbleed.py	02-Nov-2014 23:52	4.1K	
nginx_dos.py	02-Nov-2014 23:52	2.4K	
o-saft.gz	02-Nov-2014 23:52	109K	
rfi.txt	02-Nov-2014 23:52	625	
sandbox.htm	02-Nov-2014 23:52	792	
sqlite.py	02-Nov-2014 23:52	3.6K	
ssrf-1.txt	02-Nov-2014 23:52	1.4K	
ssrf-2.txt	02-Nov-2014 23:52	681	
ssrf-3.txt	02-Nov-2014 23:52	1.0K	
steal_stuff.htm	02-Nov-2014 23:52	1.6K	
xdx.as	02-Nov-2014 23:52	1.5K	
xdx.php	02-Nov-2014 23:52	768	
xdx.swf	02-Nov-2014 23:52	1.1K	
xss_steal_secret.js	02-Nov-2014 23:52	600	
xst.js	02-Nov-2014 23:52	592	

En el caso de los endpoints que contienen paneles de administración, lo más interesante a destacar es el endpoint del panel de phpMyAdmin, siendo que aún tiene la contraseña por defecto, por lo que, ingresando las claves se dispondrá de acceso y control a las bases de datos alojadas en el servidor:



Búsqueda de exploits para los servicios encontrados

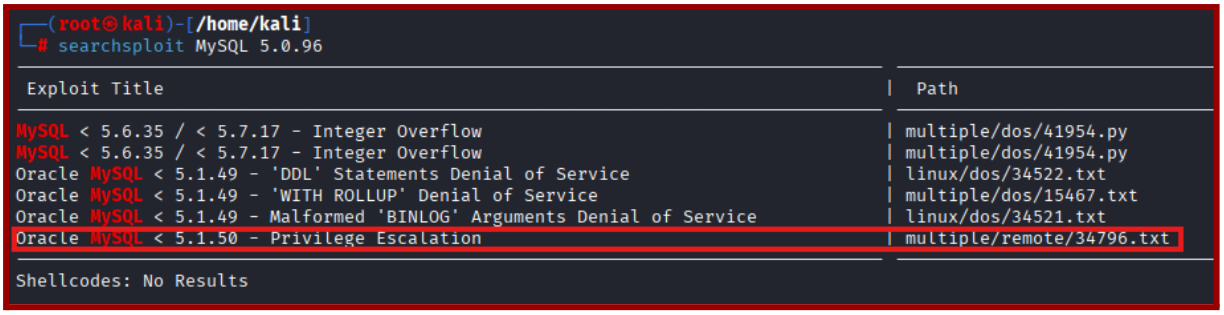
Para analizar los servicios expuestos se ha utilizado ***searchsploit***, para buscar en exploitDB los servicios que se han identificado anteriormente, al comprobar los servicios encontrados, se observan vulnerabilidades preocupantes:

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit ProFTPD 1.3
------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                  |  Path
------------------------------------------------------------------------------- ---------------------------------
ProFTPd - 'ftpdctl' 'pr_ctrls_connect' Local Overflow                           | linux/local/394.c
ProFTPd 1.2 < 1.3.0 (Linux) - 'sreplace' Remote Buffer Overflow (Metasploit)    | linux/remote/16852.rb
ProFTPd 1.3 - 'mod_sql' 'Username' SQL Injection                                | multiple/remote/32798.pl
ProFTPd 1.3.0 (OpenSUSE) - 'mod_ctrls' Local Stack Overflow                     | unix/local/10044.pl
ProFTPd 1.3.0 - 'sreplace' Remote Stack Overflow (Metasploit)                   | linux/remote/2856.pm
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (1)          | linux/local/3330.pl
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (2)          | linux/local/3333.pl
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' exec-shield Local Overflow                   | linux/local/3730.txt
ProFTPd 1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (PoC)              | linux/dos/2928.py
ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)  | linux/remote/16878.rb
ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)    | linux/remote/16851.rb
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution              | linux/remote/15662.txt
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)                       | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                             | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)                         | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                                                       | linux/remote/36742.txt
ProFTPD 1.3.7a - Remote Denial of Service                                       | multiple/dos/49697.py
ProFTPd 1.x - 'mod_tls' Remote Buffer Overflow                                  | linux/remote/4312.c
ProFTPd IAC 1.3.x - Remote Command Execution                                    | linux/remote/15449.pl
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)                        | linux/remote/16921.rb
WU-FTPD 2.4/2.5/2.6 / Trolltech ftpd 1.2 / ProFTPd 1.2 / BeroFTPD 1.3.4 FTP - glo | linux/remote/20690.sh
------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

En el caso del servicio FTP instalado, al tener una versión antigua, cuenta con una vulnerabilidad que permite la ejecución remota de comandos, así como la implantación de un backdoor, lo que hace altamente probable poder conseguir una consola remota con valores de administración.

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit OpenSSH 4.7
------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                  |  Path
------------------------------------------------------------------------------- ---------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration                                        | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                  | linux/remote/45210.py
OpenSSH < 6.6 SFTP (x64) - Command Execution                                    | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution                                          | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets P | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                        | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                            | linux/remote/45939.py
------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

En el caso de OpenSSL, se puede apreciar que también cuenta con vulnerabilidades que permiten tanto la ejecución de comandos como obtener el listado de usuario, por lo que mediante este servicio se podrían obtener credenciales de personal sin la debida autorización.



Por último, en el servicio de base de datos se aprecia que es especialmente vulnerable a las denegaciones de servicio, pero lo más preocupante es que también se puede llevar a cabo la escalada de privilegios.

Conclusión

El uso combinado con las vulnerabilidades mencionadas anteriormente, permite efectuar una escalada de privilegios mediante movimiento lateral, lo que resulta en una persona ajena con autorización de administrador, que además puede conectarse a la plataforma de manera remota con un backdoor, lo que hace que toda la información alojada en la web esté comprometida.

Una vez más, este tipo de configuraciones, con vulnerabilidades tan visibles, ponen de manifiesto la necesidad de una formación activa en el campo de la ciberseguridad.