

CURSO CIBERSEGURIDAD

Fingerprinting

Ejercicio 4

Álvaro Viera López

Contents

| | | |
|----------|-----------------------------------|----------|
| 1 | Metasploitable1 | 2 |
| 2 | Metasploitable2 | 4 |
| 3 | Servicios | 8 |
| 3.1 | SMTP (TCP/25) | 8 |
| 3.2 | DNS (TCP/53) | 8 |
| 3.3 | FTP (TCP/21) | 8 |
| 3.4 | HTTP (TCP/80) | 8 |
| 3.5 | SMB (TCP/445 y TCP/139) | 9 |
| 3.6 | MySQL (TCP/3306) | 9 |
| 3.7 | PostgreSQL (TCP/5432) | 9 |

Se va a emplear las herramientas netcat y telnet para obtener información sensible sobre los servicios/puertos abiertos de metasploitable1 y metasploitable2.

1 Metasploitable1

Netcat

```
(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 21
192.168.1.164: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.1.164] 21 (ftp) open
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.164]
^X^C sent 0, rcvd 58

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 21
(UNKNOWN) [192.168.1.164] 21 (ftp) open
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.164]
^C sent 0, rcvd 58

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 22
(UNKNOWN) [192.168.1.164] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C sent 0, rcvd 38

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 23
(UNKNOWN) [192.168.1.164] 23 (telnet) open
♦♦♦♦ ♦♦♦♦^C sent 0, rcvd 12

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 25
(UNKNOWN) [192.168.1.164] 25 (smtp) open
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
^C sent 0, rcvd 55
```

```
(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 53
(UNKNOWN) [192.168.1.164] 53 (domain) open
^X^C sent 0, rcvd 0

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 80
(UNKNOWN) [192.168.1.164] 80 (http) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 139
(UNKNOWN) [192.168.1.164] 139 (netbios-ssn) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 445
(UNKNOWN) [192.168.1.164] 445 (microsoft-ds) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 3306
(UNKNOWN) [192.168.1.164] 3306 (mysql) open
>
5.0.51a-3ubuntu5=J←jQ8b,g\v`]0w*e?MB^C sent 0, rcvd 66

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 3632
(UNKNOWN) [192.168.1.164] 3632 (distcc) open
^C sent 0, rcvd 0
```

```
(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 5432
(UNKNOWN) [192.168.1.164] 5432 (postgresql) open
^[A^[B^C sent 0, rcvd 0

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 8009
(UNKNOWN) [192.168.1.164] 8009 (?) open
^X^C sent 0, rcvd 0

(kali㉿kali)-[~]
└─$ nc -vv 192.168.1.164 8180
(UNKNOWN) [192.168.1.164] 8180 (?) open
^C sent 0, rcvd 0
```

De las imágenes podemos observar lo siguiente:

- Puerto 21: Se trata de un servicio ftp. Más específicamente, ProFTPD 1.3.1
- Puerto 22: Se trata de un servicio ssh. Más específicamente, SSH2.0OpenSSH_4.7p1
- Puerto 23: Se trata de un servicio telnet.
- Puerto 25: Se trata de un servicio smtp. Más específicamente, ESMTP Postfix. El identificador smtp es metasploitable.localdomain, donde metasploitable es el nombre de la máquina y localdomain el dominio.
- Puerto 53: Se trata de un servicio DNS.
- Puerto 80: Se trata de un servicio http.
- Puerto 139: Se trata de un servicio netbios-ssn.
- Puerto 445: Se trata de un Microsoft DS. Microsoft DS es el nombre que se le da al puerto 445 que es utilizado por SMB.

- Puerto 3306: Se trata de un servicio mysql 5.0.51a.
- Puerto 3632: Se trata de un servicio distcc.
- Puerto 5432: Se trata de un servicio postgresql.
- Los puertos 8180 y 8009 están abiertos, pero no podemos saber el servicio asociados a estos con este método.

Telnet

```
(kali@kali)-[~]
$ telnet 192.168.1.156 25
Trying 192.168.1.156 ...
Connected to 192.168.1.156.
Escape character is '^]'.
220 metasploitable.localdomain ESMTF Postfix (Ubuntu)
quit
221 2.0.0 Bye
Connection closed by foreign host.

(kali@kali)-[~]
$ telnet 192.168.1.156 53
Trying 192.168.1.156 ...
Connected to 192.168.1.156.
Escape character is '^]'.
quit
Connection closed by foreign host.

(kali@kali)-[~]
$ telnet 192.168.1.156 21
Trying 192.168.1.156 ...
Connected to 192.168.1.156.
Escape character is '^]'.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.156]
quit
221 Goodbye.
Connection closed by foreign host.
```

```
(kali@kali)-[~]
$ telnet 192.168.1.156 445
Trying 192.168.1.156 ...
Connected to 192.168.1.156.
Escape character is '^]'.
quit
```

```
(kali@kali)-[~]
$ telnet 192.168.1.156 80
Trying 192.168.1.156 ...
Connected to 192.168.1.156.
Escape character is '^]'.
quit
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>501 Method Not Implemented</title>
</head><body>
<h1>Method Not Implemented</h1>
<p>quit to /index.html not supported.<br />
</p>
<hr>
<address>Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch Server at metasploitable.localdomain Port 80</address>
</body></html>
Connection closed by foreign host.

(kali@kali)-[~]
$ telnet 192.168.1.156 3306
Trying 192.168.1.156 ...
Connected to 192.168.1.156.
Escape character is '^]'.
>
5.0.51a-3ubuntu5<G3f>7w,vi,>1y3/3R!N
quit
Connection closed by foreign host.

(kali@kali)-[~]
$ telnet 192.168.1.156 5432
Trying 192.168.1.156 ...
Connected to 192.168.1.156.
Escape character is '^]'.
quit
Connection closed by foreign host.
```

De las imágenes podemos observar lo siguiente:

- Puerto 21: Se trata de un servicio ftp. Más específicamente, ProFTPD 1.3.1
- Puerto 25: Se trata de un servicio smtp. Más específicamente, ESMTP Postfix. El identificador smtp es metasploitable.localdomain, donde metasploitable es el nombre de la máquina y localdomain el dominio.
- Puerto 53 abierto: Probablemente sea un servicio DNS.
- Puerto 80: Se trata de un servicio http.
- Puerto 445 abierto: Probablemente sea un servicio microsoft-ds.
- Puerto 3306 abierto: Probablemente sea un servicio mysql 5.0.51a.
- Puerto 5432 abierto: Probablemente sea un servicio postgresql.

Donde se han comparado los puertos abiertos sin información de servicio con la página https://es.wikipedia.org/wiki/Anexo:Puertos_de_red.

2 Metasploitable2

Netcat

```
(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 21
(UNKNOWN) [192.168.1.165] 21 (ftp) open
220 (vsFTPd 2.3.4)
^C sent 0, rcvd 20

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 22
(UNKNOWN) [192.168.1.165] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C sent 0, rcvd 38

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 23
(UNKNOWN) [192.168.1.165] 23 (telnet) open
♦♦♦♦ ♦♦♦♦^C sent 0, rcvd 12

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 25
(UNKNOWN) [192.168.1.165] 25 (smtp) open
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
^C sent 0, rcvd 55

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 53
(UNKNOWN) [192.168.1.165] 53 (domain) open
^C sent 0, rcvd 0
```

```
(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 80
(UNKNOWN) [192.168.1.165] 80 (http) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 111
(UNKNOWN) [192.168.1.165] 111 (sunrpc) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 139
(UNKNOWN) [192.168.1.165] 139 (netbios-ssn) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 445
(UNKNOWN) [192.168.1.165] 445 (microsoft-ds) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 512
(UNKNOWN) [192.168.1.165] 512 (exec) open
Where are you?
sent 0, rcvd 16

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 513
(UNKNOWN) [192.168.1.165] 513 (login) open
^C sent 0, rcvd 0
```

```

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 514
(UNKNOWN) [192.168.1.165] 514 (shell) open
sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 1099
(UNKNOWN) [192.168.1.165] 1099 (rmiregistry) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 1524
(UNKNOWN) [192.168.1.165] 1524 (ingreslock) open
root@metasploitable:/# ^C sent 0, rcvd 23

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 2049
(UNKNOWN) [192.168.1.165] 2049 (nfs) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 2121
(UNKNOWN) [192.168.1.165] 2121 (iprop) open
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.165]
^C sent 0, rcvd 58

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 3306
(UNKNOWN) [192.168.1.165] 3306 (mysql) open
>
5.0.51a-3ubuntu5xpLgBT_b,N@4$T^4.(|^C sent 0, rcvd 66

```

```

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 3632
(UNKNOWN) [192.168.1.165] 3632 (distcc) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 5432
(UNKNOWN) [192.168.1.165] 5432 (postgresql) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 5900
(UNKNOWN) [192.168.1.165] 5900 (?) open
RFB 003.003
^C sent 0, rcvd 12

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 6000
(UNKNOWN) [192.168.1.165] 6000 (x11) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 6667
(UNKNOWN) [192.168.1.165] 6667 (ircd) open
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
^C sent 0, rcvd 174

```

```

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 6697
(UNKNOWN) [192.168.1.165] 6697 (ircs-u) open
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
^C sent 0, rcvd 174

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 8009
(UNKNOWN) [192.168.1.165] 8009 (?) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 8180
(UNKNOWN) [192.168.1.165] 8180 (?) open
^C sent 0, rcvd 0

(kali㉿kali)-[~]
$ nc -vvn 192.168.1.165 8787
(UNKNOWN) [192.168.1.165] 8787 (?) open
^C sent 0, rcvd 0

```

De las imágenes podemos observar lo siguiente:

- Puerto 21: Se trata de un servicio ftp. Más específicamente, ProFTPD 2.3.4
- Puerto 22: Se trata de un servicio ssh. Más específicamente, SSH2.0OpenSSH.4.7p1
- Puerto 23: Se trata de un servicio telnet.
- Puerto 25: Se trata de un servicio smtp. Más específicamente, ESMTP Postfix. El identificador smtp es metasploitable.localdomain, donde metasploitable es el nombre de la máquina y localdomain el dominio.
- Puerto 53: Se trata de un servicio DNS.
- Puerto 80: Se trata de un servicio http.
- Puerto 111: Se trata de un servicio sunrpc.
- Puerto 139: Se trata de un servicio netbios-ssn.
- Puerto 445: Se trata de un Microsoft DS. Microsoft DS es el nombre que se le da al puerto 445 que es utilizado por SMB.
- Puerto 512: Se trata de un servicio exec.
- Puerto 513: Se trata de un servicio Rlogin.
- Puerto 514: Se trata de un servicio shell (Aunque en realidad es un servicio tcpwrapped).
- Puerto 1099: Se trata de un servicio rmiregistry.
- Puerto 1524: Se trata de un servicio ingreslock (Aunque en realidad es una bindshell)
- Puerto 2049: Se trata de un servicio nfs.
- Puerto 2121: Se trata de un servicio iprop (Aunque en realidad es un servicio ftp).
- Puerto 3306: Se trata de un servicio mysql 5.0.51a.
- Puerto 3632: Se trata de un servicio distcc.
- Puerto 5432: Se trata de un servicio postgresql.
- Puerto abierto 5900: Probablemente sea un servicio vnc.
- Puerto 6000: Se trata de un servicio x11.
- Puerto 6667: Se trata de un servicio ircd.
- Puerto 6697: Se trata de un servicio ircs-u
- Los puertos 8009, 8180 y 8787 se encuentran abiertos. Sin embargo desconocemos el servicio.

Telnet

```
[kali@kali]-[~]
$ telnet 192.168.1.149 25
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^\''.
220 metaspoitable.localdomain ESMTP Postfix (Ubuntu)
quit
221 2.0.0 Bye
Connection closed by foreign host.

[kali@kali]-[~]
$ telnet 192.168.1.149 53
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^\''.
quit
Connection closed by foreign host.

[kali@kali]-[~]
$ telnet 192.168.1.149 25
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^\''.
220 metaspoitable.localdomain ESMTP Postfix (Ubuntu)
quit
221 2.0.0 Bye
Connection closed by foreign host.

[kali@kali]-[~]
$ telnet 192.168.1.149 21
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^\''.
220 (vsFTPd 2.3.4)
quit
221 Goodbye.
Connection closed by foreign host.
```

```

$ telnet 192.168.1.149 80
Trying 192.168.1.149...
Connected to 192.168.1.149.
Escape character is '^]'.
quit
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

</pre>
<ul>
<li><a href="/twiki/">Twiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>

Connection closed by foreign host.

```

```
[kali@kali]~$
$ telnet 192.168.1.149 3306
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^]'.
>
5.0.51a-3ubuntu50918aP[>,_F)e%Zt[J]
quitConnection closed by foreign host.

[kali@kali]~$
$ telnet 192.168.1.149 5432
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^]'.
quit
Connection closed by foreign host.

    command 'quit' from deb quilt
Try: sudo apt install <deb name>
```

De las imágenes podemos observar lo siguiente:

- Puerto 21: Se trata de un servicio ftp. Más específicamente, ProFTPD 2.3.4
- Puerto 25: Se trata de un servicio smtp. Más específicamente, ESMTP Postfix. El identificador smtp es `metasploitable.localdomain`, donde `metasploitable` es el nombre de la máquina y `localdomain` el dominio.
- Puerto 53: Se trata de un servicio DNS.
- Puerto 80: Se trata de un servicio http.
- Puerto 3306 abierto: Probablemente sea un servicio mysql
- Puerto 5432 abierto: Probablemente sea un servicio postgresql.

3 Servicios

3.1 SMTP (TCP/25)

SMTP o Simple Mail Transfer Protocol es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, impresoras, etc.). Es, en otras palabras, un protocolo de conexión de Internet. Se encuentra en la capa de aplicación del modelo OSI. El funcionamiento de este protocolo se da en línea, de manera que opera en los servicios de correo electrónico. Sin embargo, este protocolo posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos). Como alternativa a esta limitación, este protocolo se ejecuta normalmente en relación con otros, por lo que este protocolo es utilizado sobre todo para enviar correos electrónicos, mientras que para la recepción se suelen utilizar otros como IMAP y POP.

La versión instalada en metasploitable1 y metasploitable2 es Postfix smtpd 2.5.1. La última versión estable es Postfix smtpd 3.5.10. Este servicio es software libre, desarrollado por Wietse Venema y otros. No se encontraron vulnerabilidades.

3.2 DNS (TCP/53)

Domain Name System o DNS es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominio asignados a cada uno de los participantes. Su función más importante es traducir nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red.

La versión instalada en metasploitable1 y metasploitable2 es ISC BIND 9.4.2, lanzada en 2009. La última versión estable es ISC BIND 9.18.7. BIND es software libre e ISC BIND, es una corporación pública caritativa sin ánimo de lucro. Si googleamos el nombre del servicio podemos encontrar varias vulnerabilidades: https://www.cvedetails.com/vulnerability-list/vendor_id-64/product_id-144/version_id-436267/ISC-Bind-9.4.2.html

3.3 FTP (TCP/21)

Las siglas de FTP significan File Transfer Protocol. Se trata de un protocolo que permite transferir archivos directamente de un dispositivo a otro que lleva 50 años con nosotros, y que es más antiguo que la propia Internet. A día de hoy todavía se utiliza en algunos contextos, aunque de cara a intercambiar archivos entre usuarios suelen utilizarse más otras alternativas como el P2P o el alojamiento en la nube.

La versión instalada en metasploitable1 es ProFTPD 1.3.1. En diciembre del 2006 se lanzó ProFTPD 1.3.1rc1. La última versión es ProFTPD 1.3.8rc4: ProFTPD es software libre y fue desarrollado por un grupo de desarrolladores (Jesse Sipprell: ProFTPD creator, MacGyver: ProFTPD maintainer, Charles Seeger, Andrew Houghton: mod_sql maintainer, Mark Lowes: Documentation and Webhamster). Si googleamos el nombre del servicio podemos encontrar varias vulnerabilidades: https://www.cvedetails.com/vulnerability-list/vendor_id-9520/product_id-16873/version_id-435968/Proftpd-Proftpd-1.3.1.html

La versión instalada en metasploitable2 es vsftpd 2.3. En julio del 2011 se descubrió que el servicio tenía una vulnerabilidad. Un usuario con una cara feliz ":)" en su nombre de usuario podía conseguir una shell en el puerto 6200. Como "solución", un atacante subió una versión actualizada, pero contenía una backdoor. La última versión de vsftpd es la 3.0.5. Es open source. Algunas vulnerabilidades aparecen recogidas en esta web: <https://repology.org/project/vsftpd/cves>

3.4 HTTP (TCP/80)

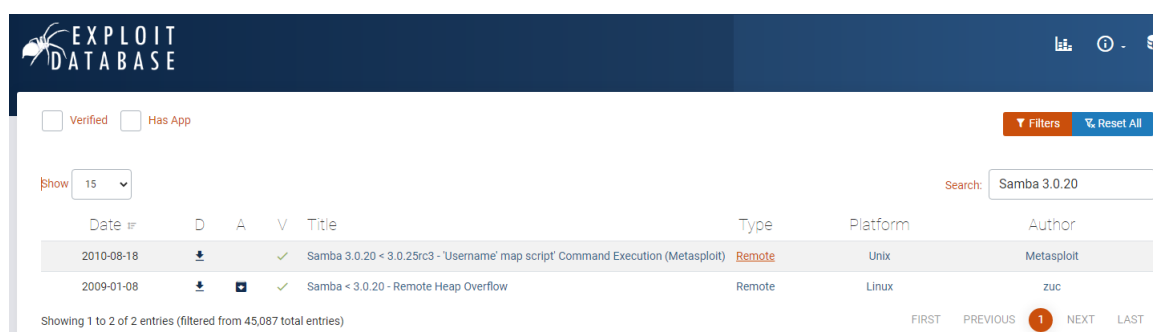
HTTP, de sus siglas en inglés: "Hypertext Transfer Protocol", es el nombre de un protocolo el cual nos permite realizar una petición de datos y recursos, como pueden ser documentos HTML. Es la base de cualquier intercambio de datos en la Web, y un protocolo de estructura cliente-servidor, esto quiere decir que una petición de datos es iniciada por el elemento que recibirá los datos (el cliente), normalmente un navegador Web.

La versión instalada en metasploitable1 y metasploitable2 es Apache httpd 2.2.8. La última versión estable es Apache httpd 2.4.53. Fue desarrollado por Apache Software Foundation. Si googlemos el nombre del servicio podemos encontrar varias vulnerabilidades: https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-416233/Apache-Http-Server-2.2.8.html

3.5 SMB (TCP/445 y TCP/139)

SMB (Server Message Block) es un protocolo cliente / servidor que gobierna el acceso a archivos y directorios completos, así como a otros recursos de red como impresoras, enrutadores o interfaces abiertas a la red. El intercambio de información entre los diferentes procesos de un sistema (también conocido como comunicación entre procesos) se puede manejar en base al protocolo SMB.

La versión instalada en metasploitable1 y metasploitable2 es netbios-ssn Samba smbd 3.0.20 lanzada en 2005. La última versión estable es Samba 4.16.0. Fue desarrollado por The Samba Team y es software libre. En Exploitdb tenemos las siguientes vulnerabilidades



The screenshot shows the Exploit Database search results for 'Samba 3.0.20'. The interface includes a search bar with the query 'Samba 3.0.20', filters for 'Verified' and 'Has App', and a 'Show' dropdown set to 15. The results table lists two entries:

| Date | D | A | V | Title | Type | Platform | Author |
|------------|---|---|---|--|--------|----------|------------|
| 2010-08-18 | | | | Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | Remote | Unix | Metasploit |
| 2009-01-08 | | | | Samba < 3.0.20 - Remote Heap Overflow | Remote | Linux | zuc |

Showing 1 to 2 of 2 entries (filtered from 45,087 total entries)

3.6 MySQL (TCP/3306)

MySQL es el sistema de gestión de bases de datos relacional más extendido en la actualidad al estar basada en código abierto. MySQL es un sistema de gestión de bases de datos que cuenta con una doble licencia. Por una parte es de código abierto, pero por otra, cuenta con una versión comercial gestionada por la compañía Oracle. MySQL presenta algunas ventajas que lo hacen muy interesante para los desarrolladores. La más evidente es que trabaja con bases de datos relacionales, es decir, utiliza tablas múltiples que se interconectan entre sí para almacenar la información y organizarla correctamente.

La versión instalada en metasploitable1 y metasploitable2 es MySQL 5.0.51a lanzada junio de 2008. La última versión es MySQL 8.0.30. En 1995 Michael Widenius desarrolló junto a David Axmark y Allan Larsson MySQL y la empresa MySQL AB. En 2008, MySQL fue adquirido por Sun Microsystems, quien en 2010 fue comprado por Oracle Corporation. Esta versión posee una RCE: <http://www.securityspace.com/es/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.100436>. Sin embargo, no posee ningún CVE asociado: https://www.cvedetails.com/vulnerability-list/vendor_id-185/product_id-316/version_id-61896/Mysql-Mysql-5.0.51a.html

3.7 PostgreSQL (TCP/5432)

PostgreSQL, o simplemente Postgres, es un sistema de código abierto de administración de bases de datos del tipo relacional, aunque también es posible ejecutar consultas que sean no relacionales. En este sistema, las consultas relacionales se basan en SQL, mientras que las no relacionales hacen uso de JSON. Dos detalles a destacar de PostgreSQL es que posee data types (tipos de datos) avanzados y permite ejecutar optimizaciones de rendimiento avanzadas, que son características que por lo general solo se ven en sistemas de bases de datos comerciales, como por ejemplo SQL Server de Microsoft u Oracle.

La versión instalada en metasploitable1 y metasploitable2 es PostgreSQL DB 8.3.0 - 8.3.7 lanzada en 2008-2009. La última versión es PostgreSQL DB 15. Como muchos otros proyectos open source, el desarrollo de PostgreSQL no es manejado por una sola compañía sino que es dirigido por una comunidad de desarrolladores y organizaciones comerciales las cuales trabajan en su desarrollo, dicha comunidad es denominada el PGDG (PostgreSQL Global Development Group). Las vulnerabilidades de la versión 8.3 vienen recogidas en la siguiente url: <https://www.postgresql.org/support/security/8.3/>. Y para la 8.3.7: https://www.cvedetails.com/vulnerability-list/vendor_id-336/product_id-575/version_id-445862/opsqli-1/Postgresql-Postgresql-8.3.7.html.