

REPORTE DE PENTEST 101

LEVEL 2 – EXAMEN



ACADEMIA DE
CIBERSEGURIDAD

Pentesting Playground 101

BIENVENIDO A TU CAMINO COMO PENTESTER

INDICE – PENTEST 101 – CIBERSEGURIDAD.**Contenido****Pág.**

1) Introducción.....	3
2) Objetivo.....	3
3) Alcance.....	3
4) Resumen Ejecutivo.....	3
5) Detalle Técnico de vulnerabilidades.....	4
6) Metodologías.....	19
7) CONCLUSION.....	20

1) Introducción:

La seguridad en todos los aspectos de la vida y más hablando en términos informáticos es esencial para mantener el orden y privacidad de la persona, es por esto que la ciberseguridad se ha convertido en un punto de importancia muy requerido en los últimos tiempos debido al gran desarrollo de tecnologías o softwares que ya forman parte del día a día en nuestra cotidianidad. Hablando sobre el campo de la ciberseguridad permite guardar y salvar la integridad, confidencialidad y disponibilidad de información tratando de prevenir o evitar las amenazas cibernéticas que siguen evolucionando y permiten nuevos desafíos diariamente.

En dicho reporte veremos con respecto al desafío “Examen de Pentesting 101”, un análisis de la información que podemos encontrar accediendo a la red donde, aplicando las técnicas correspondientes, podremos observar sus vulnerabilidades o fallas documentando todo el proceso. Procedemos entonces a explicar la metodología.

2) Objetivo:

Como objetivo se propone realizar un informe a manera de documento confidencial que pueda comprobar las vulnerabilidades o fallas encontradas en el sistema para lograr certificar el curso “Pentesting Playground 101”, encontrando las CVEs correspondientes, realizando alguna comprobación de explotación y generando una documentación ordenada a fines de evaluación.

3) Alcance:

A quien corresponda realizar dicho informe requiere para su aprobación la práctica de los conocimientos abordados en las clases, aplicando las técnicas demostradas, utilizando toda la información disponible con el uso de las herramientas aprendidas y así poner a prueba los conocimientos que posee uno mismo, generando la evidencia o pruebas necesarias de fallas o vulnerabilidades que lo demuestren.

4) Resumen Ejecutivo:

Se pone en constancia un documento informativo de las técnicas y procesos realizados mediante el acceso autorizado a través de medios informáticos digitales, buscando las distintas fallas que podrían encontrarse en sus servidores, entendiendo que al encontrarse amenazas potenciales, las mismas sean informadas con sus recomendaciones, para luego por parte de quien corresponda y lo deseé, tomar las medidas necesarias para prevenirlas adoptando prácticas más seguras y manteniéndose actualizados sobre las tendencias de la ciberseguridad.



5) Pruebas Realizadas:

Comenzamos con la parte práctica de laboratorio utilizando una VPN (virtual Private Network) proporcionada por la plataforma Tryckhackme para poder realizar una conexión remota con el servidor que será auditado.

<https://academia-ciberseguridad.com/aprende-ciberseguridad>

Luego se procede al inicio de la maquina en cuestión dentro de la plataforma otorgándonos nuestra IP cliente.

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
      inet 10.18.89.19 netmask 255.255.128.0 destination 10.18.89.19
      inet6 fe80::db8:670d:d066:98d1 prefixlen 64 scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
```

los pasos a continuación:

Reconocemos ahora la IP objetivo a la cual le realizaremos las distintas pruebas en busca de sus vulnerabilidades.

Información de la máquina activa

Título	Dirección IP	Vence	? Añadir 1 hora
Pentesting Playground 101 AC	10.10.223.126	53m 35s	Terminar

Realizamos un reconocimiento de las IP ocupadas al momento de trabajar en dicha red. Para el mismo se utilizará NMAP desde la consola de Kali Linux otorgando el rango de IP correspondiente.

```
(root㉿kali)-[~/home/kali]
# nmap 10.10.223.0-255

Nmap scan report for 10.10.223.2      Nmap scan report for 10.10.223.6
Nmap scan report for 10.10.223.23     Nmap scan report for 10.10.223.49
Nmap scan report for 10.10.223.85     Nmap scan report for 10.10.223.93
Nmap scan report for 10.10.223.125    Nmap scan report for 10.10.223.156
Nmap scan report for 10.10.223.165    Nmap scan report for 10.10.223.183
Nmap scan report for 10.10.223.197    Nmap scan report for 10.10.223.252
                                         Nmap scan report for 10.10.223.254
```

Sin desviarnos de nuestro objetivo principal IP 10.10.223.126 pasamos al análisis de la misma en cuanto a sus vulnerabilidades. Procedemos entonces a la búsqueda de algún puerto abierto que posea el mismo.

```
(root㉿kali)-[~/home/kali]
# nmap -p- 10.10.223.126
```



```

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
3306/tcp  open  mysql
8080/tcp  open  http-proxy
  
```

Se reconoce los siguientes puertos, todos abiertos, en la maquina a testear:

***FTP:** Denominado File Transfer Protocol es utilizado para la transferencia de archivos entre los sistemas, es decir permite compartir cargando o descargando archivos, ficheros, carpetas, etc. desde o hacia sus servidores a través de una conexión TCP/IP permitiendo la gestión de los múltiples archivos en entornos de red o servidores web.

- Puerto: 21

***SSH:** El protocolo Secure Shell permite mediante la cifracion la comunicación en la red de manera segura a sistemas remotos, permitiendo administrar servidores de forma remota y la gestión e intercambio a través del uso de comandos de datos entre sistemas.

- Puerto: 22

***Telnet:** Permite la comunicación bidireccional entre dos dispositivos a través de una conexión virtual, es un protocolo de red con varios años de utilización dando una comunicación de acceso remoto a sistemas que no se encuentra cifrado.

- Puerto: 23

***Http:** El Hipertext Transfer Protocol como su nombre lo dice es un protocolo de transferencia de información en la denominada World Wide Web. Es el protocolo general mas utilizado entre navegadores web y servidores para lograr su comunicación. Permite enviar ordenes de solicitud y entregas de paginas web, imágenes, videos, audios, múltiples textos, archivos, entre otros recursos.

- Puerto: 80

***Mysql:** Es uno de los sistemas mas utilizado para la gestión de base de datos relacional (RDBMS) el cual permite almacenar mediante tablas nuestra información y asi establecer un orden predeterminado de una manera mas eficiente y organizada para la fácil conexión en aplicaciones o páginas web, recuperando los datos en dicho almacenamiento.

- Puerto: 3306

***http-proxy:** Se denomina asi al servidor que funciona entre los clientes y servidores web siendo un intermediario, recibiendo las solicitudes de los clientes, envia a los servidores y luego da la respuesta que se adecue a la solicitud del mismo. En general su utilización permite una mayor eficiencia del sistema, dando rendimiento, filtrado de información y privacidad en la red.

- Puerto: 8080

A partir de dicha información realizamos un escaneo un poco más exhaustivo para localizar más información con los servicios del mismo, versiones y su sistema operativo corriente.



```
(root㉿kali)-[~/home/kali]
└─# nmap -sV -O -A 10.10.223.126
```

```
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)
| 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)
|_  256 c0:16:42:27:da:ac:56:5a:03:e3:88:22:a0:3d:86:4f (ED25519)
23/tcp    open  telnet   Linux telnetd
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Developer | Tech Enthusiast |
|_http-server-header: Apache/2.4.29 (Ubuntu)
3306/tcp  open  mysql   MySQL 5.5.23
| mysql-info:
|   Protocol: 10
|   Version: 5.5.23
|   Thread ID: 2
|   Capabilities flags: 63487
|   Some Capabilities: IgnoreSigpipes, SupportsLoadDataLocal, Support41Auth, Speaks41Pr
reSpaceBeforeParenthesis, FoundRows, SupportsCompression, LongColumnFlag, LongPassword,
tgments, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: AI-BDp'nw,rz.t"EvF7"
|_ Auth Plugin Name: mysql_native_password
8080/tcp  open  http     Apache httpd 2.4.54 ((Debian))
|_http-server-header: Apache/2.4.54 (Debian)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECT
|_http-title: Login - Adminer
No exact OS matches for host (If you know what OS is running on it, see https://nmap.or
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/14%OT=21%CT=1%CU=33240%PV=Y%DS=2%DC=T%G=Y%TM=657
OS:B5838%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10B%TI=Z%CI=Z%TS=A)SEQ(
OS:SP=103%GCD=1%ISR=10C%TI=Z%CI=Z%TS=A)OPS(O1=M509ST11NW6%O2=M509ST11NW6%O3
```

```
OS:=M509NNT11NW6%O4=M509ST11NW6%O5=M509ST11NW6%O6=M509ST11)WIN(W1=F4B3%W2=F
OS:4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M509NNSNW
OS:6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Se reconoce un sistema Operativo **LINUX**, AHORA pasamos entonces al reconocimiento de los diferentes puertos con respecto a sus versiones a ver que encontramos:

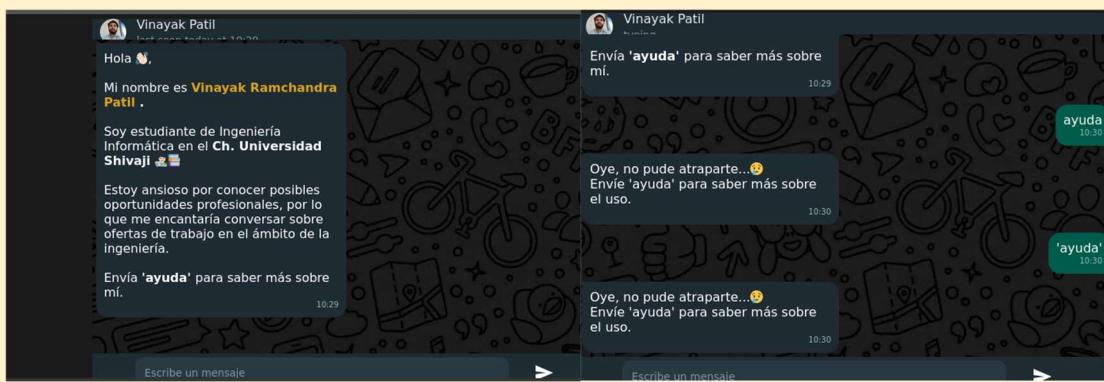
0) RECONOCIMIENTO GENERAL:

Se procede a realizar una búsqueda de la información sensible que podría verse expuesta con el solo hecho de tener un acceso a la red. Realizamos un whatweb para reconocimiento de la misma.

```
http:// 10.10.223.126 200 OK Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ub
untu Linux][Apache/2.4.29 (Ubuntu)], IP[10.10.73.197], Open-Graph-Protocol[website], Scr
ipt, Title[Developer | Tech Enthusiast |], X-UA-Compatible[IE=edge]
```

Entramos al puerto 80, vemos un simulador de chat de Whatsapp donde se involucra a una persona llamada VINAYAK PATIL, allí encontramos nombre completo y alguna información relevante de estudio. Tenemos la posibilidad de mandar mensajes pero este no nos captura.





Módulo de WHATSAPP: <https://github.com/vinayak-09>

Por otro lado también se hizo un DIRB para ver directorios y se encontraron 2 que son el de "images" y "assets".

```
— Scanning URL: http://10.10.223.126 —
OffSec PruebaHackMe | Caja f... Cuentas VPN gratuitas...
⇒ DIRECTORY: http://10.10.223.126/assets/
⇒ DIRECTORY: http://10.10.223.126/images/
+http://10.10.223.126/index.html (CODE:200|SIZE:3836)
+http://10.10.223.126/server-status (CODE:403|SIZE:277)

--- Entering directory: http://10.10.223.126/assets/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://10.10.223.126/images/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
```

En el de imágenes podemos ver las diferentes imágenes utilizadas para la aplicación WPP e iconos, como también alguna información mas personal del mismo VINAYAK.

Índice de /imágenes			
Nombre	Última modificación	Tamaño	Descripción
directorio de padres		-	
 bg.webp	2023-12-09 02:55	68K	
 chatbot.png	2023-12-09 02:55	26K	
 demo.gif	2023-12-09 02:55	2,4 millones	
 descargarIcon.svg	2023-12-09 02:55	331	
 dp.jpg	2023-12-09 02:55	16K	
 github.svg	2023-12-09 02:55	814	
 gmail.svg	2023-12-09 02:55	404	
 iconos8-cerrar.svg	2023-12-09 02:55	597	
 instagram.svg	2023-12-09 02:55	1.1K	
 linkedin.svg	2023-12-09 02:55	424	
 pdf.png	2023-12-09 02:55	10K	

Vinayak Patil
Computer Science Engineer

To pursue a job opportunity in a competitive environment that will challenge me to push my boundaries and expand my knowledge in the field of computer science while allowing me to add value to the dynamics of the company.

pushm777@gmail.com
Kothapet, India
quora.com/profile/Vinayak-Patil-17

+91 8600765857
linkedin.com/in/vinayak-patil-793bb5206
github.com/vinayak-09

EDUCATION
B.Tech in Computer Science Engineering
Tatyasaheb Kore Institute of Engineering & Technology
80CGPA - First Year

SKILLS
Java Python Flutter ReactJS C C++
JavaScript

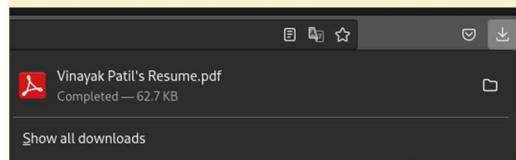
PDF



En la parte de Assets existe una información adicional y el CV con información personal del mismo VINAYAK pero mas completa y descargable como vemos en pdf.

Index of /assets

Name	Last modified	Size	Description
 Parent Directory			
 Vinayak Patil's Resume.pdf	2023-12-09 02:55	63K	
 sentmessage.mp3	2023-12-09 02:55	9.0K	



Revisando ahora el puerto 8080 podemos ver el ingreso a una base de datos MySQL en la cual nos pide la siguiente serie de datos para poder ingresar:

Idioma: Español

Administrador 4.7.8

Acceso

El fichero o directorio no existe

Motor de base de datos	mysql
Servidor	servidor local
Usuario	<input type="text"/>
Contraseña	<input type="password"/>
Base de datos	<input type="text"/>

Acceso Guardar contraseña

En el puerto 3306 podemos ver una pagina que quedo allí posee una información encriptada pero no del todo.

Inspeccionando un poco la pagina ahora en su código podemos ver las solicitudes allí o cookies unos sectores llamados Admin_key y Adminer_sid.

Name	Value
adminer_key	d4083982e61a...
adminer_permanent	
adminer_sid	13d6a361dc4dcde63858f703b97fc513
adminer_version	4.8.1

Desencriptamos entonces identificamos el HASH primero y nos dio un MD5.

Creamos un fichero llamado “cpj2.txt” entonces con dicho hash y aplicando hashcat vemos que podemos encontrar aplicando el diccionario rockyou.txt

```
(root㉿kali)-[~/home/kali]
# hashcat -m 0 cpj2.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, REL0C, SPIR, LLVM 15.0.7, S
LEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-sandybridge-Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 3483/7030 MB (10
24 MB allocatable), 5MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode....: 0 (MD5)
Hash.Target....: 1862b2b5f113710bdd1891c16b9c41e8
Time.Started....: Mon Dec 18 13:42:10 2023 (3 secs)
Time.Estimated ...: Mon Dec 18 13:42:13 2023 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 5593.5 kH/s (0.11ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 14344385/14344385 (100.00%)
Rejected.....: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[21214654412121] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1 ..: Util: 30%
```

Nos encuentra que el mismo esta en HEX entonces pasamos a descodificar también:

Candidates.#1....: \$HEX[21214654412121] → \$HEX[042a0337c2a156616d6f732103]

Pegue el texto que desea decodificar hexagonal aquí:

Hex al texto Descargar archivo

Copie el hexagonal decodificado texto aquí:

Aquí se muestra el resultado en pantalla vemos que no nos da un resultado aceptable, esto se probó para ambos casos de Admin.

1) Servicio FTP (Versión vsftpd 3.0.3)

PORT	STATE	SERVICE	VERSION	bound 101 AC	10.10.223.126
21/tcp	open	ftp	vsftpd 3.0.3		

Encontramos la versión vsftpd 3.0.3 del mismo, procedemos entonces a tratar de entrar con el logeo realizado por defecto como usuario Anonymous. Observamos que posee una configuración de usuario programada por lo que nos da “login failed”.



```
(root㉿kali)-[~/home/kali]
# ftp 10.10.223.126
Connected to 10.10.223.126.
220 (vsFTPD 3.0.3)
Name (10.10.223.126:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> 
```

Corroborado esto ahora si nos ponemos a trabajar con la versión vsftpd 3.0.3 tratando de buscar alguna falla que tenga la misma. Realizando la búsqueda manual ingresamos a la pagina <https://www.exploit-db.com/> y buscando su versión encontramos un resultado.

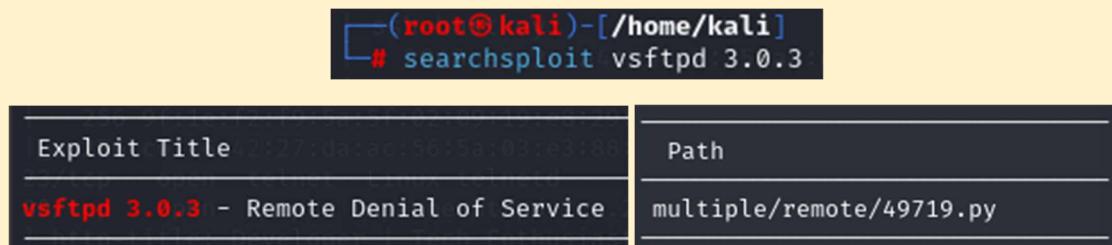


Date	D	A	V	Title	Type	Platform	Author
2021-03-29				✓ vsftpd 3.0.3 - Remote Denial of Service	Remote	Multiple	xynmaps

2021-03-29  ✓ vsftpd 3.0.3 - Remote Denial of Service

Vemos aquí un Exploit de Ataque tipo DOS a la versión en la que nos encontramos, pudiendo lograrse un ataque distribuido de Denegación de Servicio comprometiendo al sistema, inundando su servicio o red con el tráfico que queramos, teniendo como objetivo principal sobrecargarlo y hacerlo inaccesible para usuarios legítimos.

Procedemos a la búsqueda del exploit en nuestra consola.



```
(root㉿kali)-[~/home/kali]
# searchsploit vsftpd 3.0.3
```

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

2) Servicio SSH (Version OpenSSH 7.6p1)

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

Procedemos entonces ahora a realizar el mismo procedimiento, se reconoce entonces que para dicha versión de OpenSSH 7.6.p1 se encuentra una vulnerabilidad con exploit creado en Python que permite la enumeración de usuarios, esto significa que da información presente del sistema que identifican a usuarios únicos perdiendo su confidencialidad.



EXPLOIT DATABASE

Verificado Tiene aplicación

Filtros Resetear todo

Espectáculo 15

Buscar: OpenSSH

Fecha	D	A	V	Título	Tipo	Plataforma	Autor
2019-01-11	↓	✗		Cliente OpenSSH SCP: escribir archivos arbitrarios	Remoto	Múltiple	de Harry Sinton
2018-12-04	↓	✗		OpenSSH < 7.7 - Enumeración de usuarios (2)	Remoto	linux	Salto de seguridad
2018-08-21	↓	✓		OpenSSH 2.3 < 7.7 - Enumeración de nombres de usuario	Remoto	linux	Justin Gardner
2018-08-16	↓	✓		OpenSSH 2.3 < 7.7 - Enumeración de nombres de usuario (PoC)	Remoto	linux	Mateo Daley

Esto es una vulnerabilidad grave, ya que de forma remota y sin autorización permite acceso a información de la infraestructura y teniendo el nombre de usuario y con el correcto ataque de fuerza bruta de contraseñas podrá obtener un acceso al sistema.

```
(root㉿kali)-[~/home/kali/Downloads]# searchsploit OpenSSH 7.6p1
Exploit Title
OpenSSH 2.3 < 7.7 - Username Enumeration
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSH < 7.7 - User Enumeration (2)
Path
linux/remote/45233.py
linux/remote/45210.py
linux/remote/45939.py
```

3) Servicio Telnet (23/tcp)

23/tcp open telnet Linux telnetd

```
(root㉿kali)-[~/home/kali]# searchsploit telnet linux telnetd
Exploit Title
netkit-telnet-0.17 telnetd (Fedora 31) - 'BraveStarr' Remote Code Execution
telnetd encrypt_keyid - Function Pointer Overwrite
Shellcode Title
Linux/MIPS (Little Endian) - system(telnetd -l /bin/sh) Shellcode (80 bytes)
Path
linux/remote/48170.py
linux/remote/18280.c
Path
linux_mips/27132.txt
```

Vemos que encontramos un exploit y un Shellcode Tittle para la versión de Telnetd pero en la versión de Fedora 31 de netkit-telnet-0.17 telnetd que es explotable remotamente, pero no todas las distribuciones Linux son susceptibles a la misma, dicho es el caso. La otra vulnerabilidad es un desbordamiento de búfer a través del puerto TCP 5916, tampoco acopla al caso.

EXPLOIT DATABASE

Verificado Tiene aplicación

Filtros Resetear todo

Espectáculo 15

Buscar: telnet linux telnetd

Fecha	D	A	V	Título	Tipo	Plataforma	Autor
No se encontraron registros coincidentes							

Probamos un inicio de sesión a la misma para ver si posee su determinación de usuario y contraseña por defecto.

A continuación vemos que esto no es así:



```
(root㉿kali)-[~/home/kali]
# telnet 10.10.223.126
Trying 10.10.223.126 ...

Escape character is '^]'.
Ubuntu 18.04.6 LTS
ubuntu login: root

Login incorrect
ubuntu login: 
```

4) Servicio http (80/tcp)

```
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Developer | Tech Enthusiast |
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

Exploit Title	Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin	php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote C	php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl grace	linux/local/46676.php
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial o	multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck	unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck	unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck	unix/remote/764.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP'	linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory	multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory	multiple/remote/6229.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory	unix/remote/14489.c
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 /	jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 /	windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denia	linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local	linux/remote/34.pl

Se ven versiones en la que este servicio Apache se encuentra, el mismo no posee la última versión posee muchas vulnerabilidades, algunas de SSL, DOS o de control remoto del sistema.

EXPLOIT DATABASE						
<input type="checkbox"/> Verificado <input type="checkbox"/> Tiene aplicación		<input type="checkbox"/> Filtros <input type="checkbox"/> Resetear todo				
Espectáculo	15	Fecha	D	A	V	Título
2023-04-01		✓	Apache 2.4.x: desbordamiento de búfer			Aplicaciones web Múltiple Sunil Iyengar
2021-11-11		✓	Servidor HTTP Apache 2.4.50: ejecución remota de código (RCE) (3)			Aplicaciones web Múltiple Valentin Lobstein
2021-10-25		✗	Servidor HTTP Apache 2.4.50: ejecución remota de código (RCE) (2)			Aplicaciones web Múltiple El último VV
2021-10-13		✓	Servidor HTTP Apache 2.4.50: recorrido de ruta y ejecución remota de código (RCE)			Aplicaciones web Múltiple Lucas Sousa
2021-10-06		✓	Servidor Apache HTTP 2.4.49: recorrido de ruta y ejecución remota de código (RCE)			Aplicaciones web Múltiple Lucas Sousa
2019-04-08		✗	Apache 2.4.17 < 2.4.38 - Escalada de privilegios locales 'apache2ctl elegante' 'logrotate'			Local linux cfreal
2017-09-18		✗	Apache < 2.2.34 / < 2.4.27 - OPCIONES Pérdida de memoria			Aplicaciones web linux tienen bock
2016-12-12		✗	Apache 2.4.23 mod_http2 - Denegación de servicio			Del linux Jungun Baek



5) Servicio MySQL 5.5.23 (3306/tcp)

```
3306/tcp open mysql MySQL 5.5.23
| mysql-info:
|   Protocol: 10
|   Version: 5.5.23
|   Thread ID: 2
```

(root㉿kali)-[~/home/kali]		Buscar mysql 5.5.
Exploit Title	Tipo	Path
MySQL / MariaDB / PerconaDB 5.5.51/5.6.32/5	linux/local/40360.py	David Golunski
MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7	linux/local/40678.c	David Golunski
MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7	linux/local/40679.sh	David Golunski
MySQL 5.5.45 (x64) - Local Credentials Disclosure	windows_x86-64/local/40337.py	
MySQL 5.5.45 - procedure analyse Function Disclosure	multiple/dos/39867.py	
MySQL 5.5.8 - Remote Denial of Service	windows/dos/18269.py	David Golunski
MySQL < 5.6.35 / < 5.7.17 - Integer Overflow	multiple/dos/41954.py	
MySQL < 5.6.35 / < 5.7.17 - Integer Overflow	multiple/dos/41954.py	Yakir Wizman

Aquí vemos que buscando por la versión de la base de datos encontramos todas estas vulnerabilidades que podrían estar presentes por falta de actualización, si bien la base es MySQL 5.5.23, vemos allí exploits de versiones anteriores y de la presente de ataque de DOS, credenciales y locales.

EXPLOIT DATABASE			
Espectáculo	15	Buscar:	mysql 5.5
Fecha	D	A	V Título
2016-11-01	↓	X	MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7.x - Escalada de privilegios de usuario del sistema 'root'
2016-11-01	↓	X	MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7.x - Escalada de privilegios de usuario del sistema 'mysql'/Condición de carrera
2016-09-12	↓	X	MySQL / MariaDB / PerconaDB 5.5.51/5.6.32/5.7.14 - Ejecución de código/Escalamiento de privilegios
2016-09-05	↓	X	MySQL 5.5.45 (x64): divulgación de credenciales locales
2016-05-30	↓	X	MySQL 5.5.45: procedimiento de análisis de función de denegación de servicio
2011-12-24	↓	X	MySQL 5.5.8: Denegación de servicio remota
2016-11-01	↓	X	MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7.x - Escalada de privilegios de usuario del sistema 'root'
2016-11-01	↓	X	MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7.x - Escalada de privilegios de usuario del sistema 'mysql'/Condición de carrera
2016-09-12	↓	X	MySQL / MariaDB / PerconaDB 5.5.51/5.6.32/5.7.14 - Ejecución de código/Escalamiento de privilegios
2016-09-05	↓	X	MySQL 5.5.45 (x64): divulgación de credenciales locales
2016-05-30	↓	X	MySQL 5.5.45: procedimiento de análisis de función de denegación de servicio
2011-12-24	↓	X	MySQL 5.5.8: Denegación de servicio remota

6) Servicio http (8080/tcp)

```
8080/tcp open http Apache httpd 2.4.54 ((Debian))
|_http-server-header: Apache/2.4.54 (Debian)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECT
|_http-title: Login - Adminer
```



Exploit Title	Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin R	php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Co	php/remote/29316.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of	multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.	unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV	unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV	unix/remote/764.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP'	linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory L	multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory T	multiple/remote/6229.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory T	unix/remote/14489.c
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / <	jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / <	windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial	linux/dos/36906.txt
Webroot Shoutbox < 2.32 (Apache) - Local F	linux/remote/34.pl

Se ven versiones en la que este servicio Apache se encuentra, el mismo no posee la última versión posee muchas vulnerabilidades, algunas de SSL, DOS o de control remoto del sistema.

Además al estar corriendo Adminer se buscó sobre su versión ADMINER 4.7.8 /4.8.1 vemos que la versión no corresponde a vulnerabilidades.

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

EXPLOIT DATABASE																																																																																																								
<input type="checkbox"/> Verificado	<input type="checkbox"/> Tiene aplicación	<input type="checkbox"/> Filtros	<input type="checkbox"/> Resetear todo	Buscar:	apache 2.4.																																																																																																			
<table border="1"> <thead> <tr> <th>Espectáculo</th> <th>15</th> <th>Filtrar</th> </tr> <tr> <th>Fecha</th> <th>D</th> <th>A</th> <th>V</th> <th>Título</th> <th>Tipo</th> <th>Plataforma</th> <th>Autor</th> </tr> </thead> <tbody> <tr> <td>2023-04-01</td> <td>+</td> <td>✓</td> <td></td> <td>Apache 2.4.x: desbordamiento de búfer</td> <td>Aplicaciones web</td> <td>Múltiple</td> <td>Sunil Iyengar</td> </tr> <tr> <td>2021-11-11</td> <td>+</td> <td>✓</td> <td></td> <td>Servidor HTTP Apache 2.4.50: ejecución remota de código (RCE) (3)</td> <td>Aplicaciones web</td> <td>Múltiple</td> <td>Valentin Lobstein</td> </tr> <tr> <td>2021-10-25</td> <td>+</td> <td>✗</td> <td></td> <td>Servidor HTTP Apache 2.4.50: ejecución remota de código (RCE) (2)</td> <td>Aplicaciones web</td> <td>Múltiple</td> <td>El último VVV</td> </tr> <tr> <td>2021-10-13</td> <td>+</td> <td>✓</td> <td></td> <td>Servidor HTTP Apache 2.4.50: recorrido de ruta y ejecución remota de código (RCE)</td> <td>Aplicaciones web</td> <td>Múltiple</td> <td>Lucas Sousa</td> </tr> <tr> <td>2021-10-06</td> <td>+</td> <td>✗</td> <td>✓</td> <td>Servidor Apache HTTP 2.4.49: recorrido de ruta y ejecución remota de código (RCE)</td> <td>Aplicaciones web</td> <td>Múltiple</td> <td>Lucas Sousa</td> </tr> <tr> <td>2019-04-08</td> <td>+</td> <td>✗</td> <td></td> <td>Apache 2.4.17 < 2.4.38 - Escalada de privilegios locales 'apache2ctl elegante' 'logrotate'</td> <td>Local</td> <td>linux</td> <td>cfreal</td> </tr> <tr> <td>2017-09-18</td> <td>+</td> <td>✗</td> <td></td> <td>Apache < 2.2.34 / < 2.4.27 - OPCIONES Pérdida de memoria</td> <td>Aplicaciones web</td> <td>linux</td> <td>tienien bock</td> </tr> <tr> <td>2016-12-12</td> <td>+</td> <td>✗</td> <td>✓</td> <td>Apache 2.4.23 mod_http2 - Denegación de servicio</td> <td>Def</td> <td>linux</td> <td>Jungun Baek</td> </tr> <tr> <td>2016-02-01</td> <td>+</td> <td>✗</td> <td></td> <td>Apache 2.4.7 + PHP 7.0.2 - Ejecución de código de memoria no inicializado 'openssl_seal()'</td> <td>Remoto</td> <td>PHP</td> <td>akat1</td> </tr> <tr> <td>2015-12-18</td> <td>+</td> <td>✓</td> <td></td> <td>Apache 2.4.17 - Denegación de servicio</td> <td>Def</td> <td>ventanas</td> <td>rUnViRuS</td> </tr> <tr> <td>2014-07-21</td> <td>+</td> <td>✗</td> <td></td> <td>Apache 2.4.7 mod_status - Condición de carrera de manejo del marcador</td> <td>Def</td> <td>linux</td> <td>Marek Kromeke</td> </tr> </tbody> </table>						Espectáculo	15	Filtrar	Fecha	D	A	V	Título	Tipo	Plataforma	Autor	2023-04-01	+	✓		Apache 2.4.x: desbordamiento de búfer	Aplicaciones web	Múltiple	Sunil Iyengar	2021-11-11	+	✓		Servidor HTTP Apache 2.4.50: ejecución remota de código (RCE) (3)	Aplicaciones web	Múltiple	Valentin Lobstein	2021-10-25	+	✗		Servidor HTTP Apache 2.4.50: ejecución remota de código (RCE) (2)	Aplicaciones web	Múltiple	El último VVV	2021-10-13	+	✓		Servidor HTTP Apache 2.4.50: recorrido de ruta y ejecución remota de código (RCE)	Aplicaciones web	Múltiple	Lucas Sousa	2021-10-06	+	✗	✓	Servidor Apache HTTP 2.4.49: recorrido de ruta y ejecución remota de código (RCE)	Aplicaciones web	Múltiple	Lucas Sousa	2019-04-08	+	✗		Apache 2.4.17 < 2.4.38 - Escalada de privilegios locales 'apache2ctl elegante' 'logrotate'	Local	linux	cfreal	2017-09-18	+	✗		Apache < 2.2.34 / < 2.4.27 - OPCIONES Pérdida de memoria	Aplicaciones web	linux	tienien bock	2016-12-12	+	✗	✓	Apache 2.4.23 mod_http2 - Denegación de servicio	Def	linux	Jungun Baek	2016-02-01	+	✗		Apache 2.4.7 + PHP 7.0.2 - Ejecución de código de memoria no inicializado 'openssl_seal()'	Remoto	PHP	akat1	2015-12-18	+	✓		Apache 2.4.17 - Denegación de servicio	Def	ventanas	rUnViRuS	2014-07-21	+	✗		Apache 2.4.7 mod_status - Condición de carrera de manejo del marcador	Def	linux	Marek Kromeke
Espectáculo	15	Filtrar																																																																																																						
Fecha	D	A	V	Título	Tipo	Plataforma	Autor																																																																																																	
2023-04-01	+	✓		Apache 2.4.x: desbordamiento de búfer	Aplicaciones web	Múltiple	Sunil Iyengar																																																																																																	
2021-11-11	+	✓		Servidor HTTP Apache 2.4.50: ejecución remota de código (RCE) (3)	Aplicaciones web	Múltiple	Valentin Lobstein																																																																																																	
2021-10-25	+	✗		Servidor HTTP Apache 2.4.50: ejecución remota de código (RCE) (2)	Aplicaciones web	Múltiple	El último VVV																																																																																																	
2021-10-13	+	✓		Servidor HTTP Apache 2.4.50: recorrido de ruta y ejecución remota de código (RCE)	Aplicaciones web	Múltiple	Lucas Sousa																																																																																																	
2021-10-06	+	✗	✓	Servidor Apache HTTP 2.4.49: recorrido de ruta y ejecución remota de código (RCE)	Aplicaciones web	Múltiple	Lucas Sousa																																																																																																	
2019-04-08	+	✗		Apache 2.4.17 < 2.4.38 - Escalada de privilegios locales 'apache2ctl elegante' 'logrotate'	Local	linux	cfreal																																																																																																	
2017-09-18	+	✗		Apache < 2.2.34 / < 2.4.27 - OPCIONES Pérdida de memoria	Aplicaciones web	linux	tienien bock																																																																																																	
2016-12-12	+	✗	✓	Apache 2.4.23 mod_http2 - Denegación de servicio	Def	linux	Jungun Baek																																																																																																	
2016-02-01	+	✗		Apache 2.4.7 + PHP 7.0.2 - Ejecución de código de memoria no inicializado 'openssl_seal()'	Remoto	PHP	akat1																																																																																																	
2015-12-18	+	✓		Apache 2.4.17 - Denegación de servicio	Def	ventanas	rUnViRuS																																																																																																	
2014-07-21	+	✗		Apache 2.4.7 mod_status - Condición de carrera de manejo del marcador	Def	linux	Marek Kromeke																																																																																																	
<table border="1"> <thead> <tr> <th>Espectáculo</th> <th>15</th> <th>Filtrar</th> </tr> <tr> <th>Fecha</th> <th>D</th> <th>A</th> <th>V</th> <th>Título</th> <th>Tipo</th> <th>Plataforma</th> <th>Autor</th> </tr> </thead> <tbody> <tr> <td>2018-01-15</td> <td>+</td> <td>✗</td> <td></td> <td>Adminer 4.3.1: falsificación de solicitudes del lado del servidor</td> <td>Aplicaciones web</td> <td>PHP</td> <td>hip3rlinx</td> </tr> </tbody> </table>						Espectáculo	15	Filtrar	Fecha	D	A	V	Título	Tipo	Plataforma	Autor	2018-01-15	+	✗		Adminer 4.3.1: falsificación de solicitudes del lado del servidor	Aplicaciones web	PHP	hip3rlinx																																																																																
Espectáculo	15	Filtrar																																																																																																						
Fecha	D	A	V	Título	Tipo	Plataforma	Autor																																																																																																	
2018-01-15	+	✗		Adminer 4.3.1: falsificación de solicitudes del lado del servidor	Aplicaciones web	PHP	hip3rlinx																																																																																																	
<table border="1"> <thead> <tr> <th>Fecha</th> <th>D</th> <th>A</th> <th>V</th> <th>Título</th> </tr> </thead> <tbody> <tr> <td>2018-01-15</td> <td>+</td> <td>✗</td> <td></td> <td>Adminer 4.3.1: falsificación de solicitudes del lado del servidor</td> </tr> </tbody> </table>						Fecha	D	A	V	Título	2018-01-15	+	✗		Adminer 4.3.1: falsificación de solicitudes del lado del servidor																																																																																									
Fecha	D	A	V	Título																																																																																																				
2018-01-15	+	✗		Adminer 4.3.1: falsificación de solicitudes del lado del servidor																																																																																																				



6) Detalle Técnico de las Vulnerabilidades:

1) **Servicio FTP (21/tcp) – Puerto: 21 – FTP (Versión vsftpd 3.0.3) - CVE -2015-1419.**

Elemento Afectado	
10.10.223.126:21/TCP	
Propuesta de explotación	Sí

Categoría	Valor
Clasificación base	7.5
Temporalidad	N/A
Ambiente de explotación	8.0
Severidad total	8.0

CVSS v3.0

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

**Evidencia:

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

CVE -2015-1419

Se observa efectivamente que el exploit correspondiente de ataque denominado DOS esta presente en dicho puerto debido a su desactualización. La versión con la que se encuentra permite que personas ajena que requieran el ataque al sistema, mediante el colapso del mismo enviando muchas peticiones, aprovechen esta brecha creada para poder evitar algunos protocolos de seguridad o limitaciones restrictivas del sistema para poder interactuar y llevar a cabo actividades no permitidas a atacantes.

**Recomendaciones:

- Vulnerabilidad #1: Respecto al servicio FTP se debe de realizar la búsqueda de su última actualización del servicio e instalar la versión más reciente corrigiendo la misma.

Referencia – CVE-2015-1419:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1419>

<http://www.securityspace.com/es/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.108045>

<https://access.redhat.com/security/cve/cve-2015-1419>

<https://www.cvedetails.com/cve/CVE-2015-1419/>



2) Servicio SSH (22/tcp) – Puerto: 22 – SSH (Version OpenSSH 7.6p1)- CVE -2018-15473

Elemento Afectado	
10.10.223.126:22/TCP	
Propuesta de explotación	Sí

Categoría	Valor
Clasificación base	8.2
Temporalidad	7.3
Ambiente de explotación	7.4
Severidad total	7.4

CVSS:3.0

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

****Evidencia:**

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 < 7.7 - User Enumeration (2)	linux/remote/45939.py


```
(root㉿kali)-[~/Desktop/CVE-2018-15473]
# ./CVE-2018-15473.py 10.10.223.126 -u admin
[-] admin is an invalid username

(root㉿kali)-[~/Desktop/CVE-2018-15473]
# ./CVE-2018-15473.py 10.10.223.126 -u root
[+] root is a valid username

(root㉿kali)-[~/Desktop/CVE-2018-15473]
# ./CVE-2018-15473.py 10.10.223.126 -u vinayak
[-] vinayak is an invalid username

(root㉿kali)-[~/Desktop/CVE-2018-15473]
# ./CVE-2018-15473.py 10.10.223.126 -u ramchandra
[-] ramchandra is an invalid username

(root㉿kali)-[~/Desktop/CVE-2018-15473]
# 
```

CVE -2018-15473

El servicio OpenSSH desde las versiones inferiores a la 7.7 permite una enumeración de usuarios debido a que en el proceso de autenticación las solicitudes no existe un retraso de respuesta al probar intentos de autenticación inválidos hasta después de analizarse completamente el paquete que posee dicha solicitud. Esto quiere decir que está fallando en los protocolos de seguridad del servicio vinculando a los archivos nombrados en general con “auth” o “hostbased”.

****Recomendaciones:**

- Vulnerabilidad #2: Respecto al servicio SSH se debe de realizar la búsqueda de su última actualización del servicio e instalar la versión más reciente corrigiendo la misma.
- Utilización de Usuarios y contraseñas seguras (12 caracteres con minúsculas, mayúsculas, números y símbolos) con configuración robusta y no por defecto como administrador o usuario root.

Referencia – CVE-2018-15473:

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

<https://www.hackplayers.com/2018/10/enumeracion-de-usuarios-openssh.html>

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



3) Servicio HTTP-proxy (8080/tcp) – Puerto: 8080 – Apache 2.4.54- CVE-2023-25690

Elemento Afectado	
10.10.223.126:8080/TCP	
Propuesta de explotación	Sí

Categoría	Valor
Clasificación base	9.8
Temporalidad	8.8
Ambiente de explotación	7.5
Severidad total	7.5

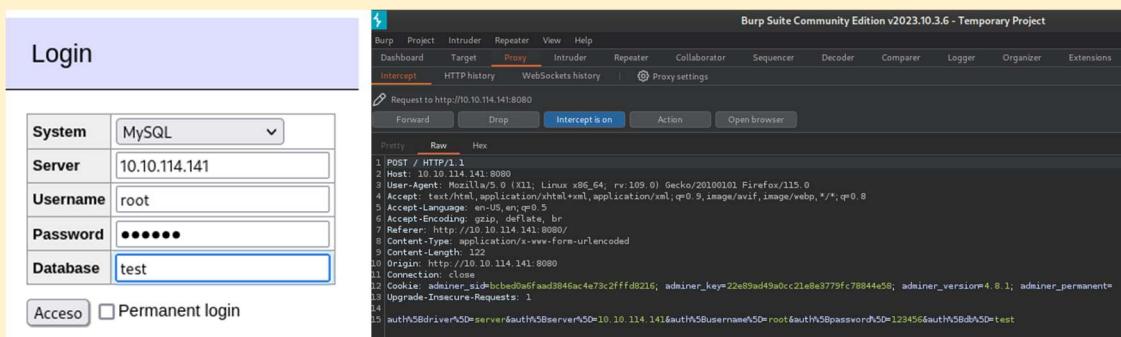
CVSS v3.0

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

****Evidencia:**

```
└──(root㉿kali)-[~/home/kali]
  # searchsploit apache 2.4.54
Exploit Title | Path
-----|-----
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin R | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Co | php/remote/29316.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.' | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV' | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV' | unix/remote/764.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory L | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory T | multiple/remote/6229.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory T | unix/remote/14489.c
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial | linux/dos/36906.txt
Webroot Shoutbox < 2.32 (Apache) - Local F | linux/remote/34.pl
```

Se procedió en dicho panel a completarlo e interceptar su solicitud por Burpsuite en proxy.



The screenshot shows the Burp Suite interface with the "Proxy" tab selected. In the "Raw" section of the message editor, the following POST request is displayed:

```
POST / HTTP/1.1
Host: 10.10.114.141:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Referer: http://10.10.114.141:8080/
Content-Type: application/x-www-form-urlencoded
Content-Length: 122
Origin: http://10.10.114.141:8080
Connection: close
Cookie: adminer_sid=bcbed0af6faad845ac4e73c2fffd8216; adminer_key=22e89ad49a0cc21e8e3779fc78844e50; adminer_version=4.8.1; adminer_permanent=1
Upgrade-Insecure-Requests: 1
auth%5Bdriver%5D=server&auth%5Bse...
```

Vemos entonces que nos da el numero “1” en la solicitud, para darnos acceso colocamos entonces un “0” para el acceso permitido seguro.

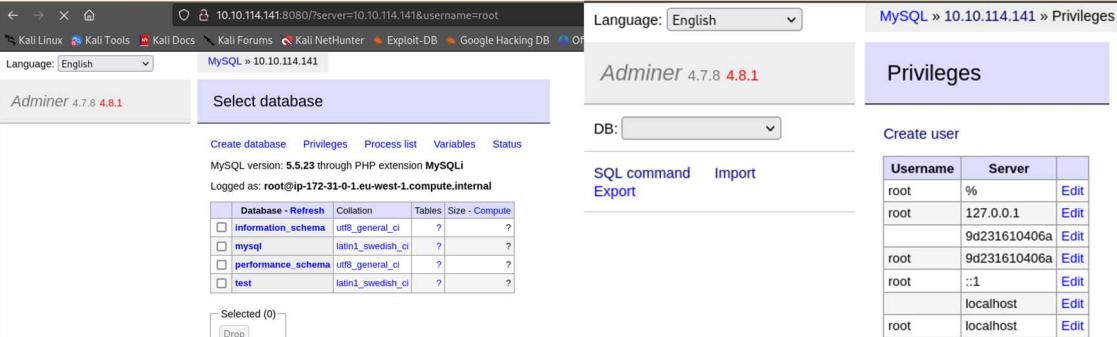


The screenshot shows two terminal windows side-by-side. The left window shows the original request with the header "Upgrade-Insecure-Requests: 1". The right window shows the modified request where the value has been changed to "0".

Mandamos la petición y vemos que ingresamos a la base de datos, y podemos ver sus tablas como tambien manipularlas.

Notamos que nos reconoce como usuario root, con la ip correspondiente a la pagina y permite ver distinta informacion.

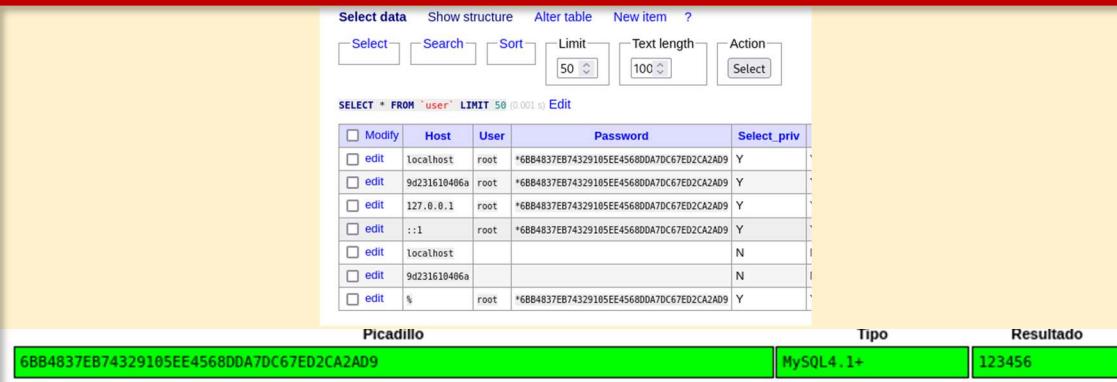




The screenshot shows the Adminer interface for MySQL version 5.5.23. The left panel displays the 'Select database' screen with databases like information_schema, mysql, performance_schema, and test. The right panel shows the 'Privileges' section with a table of users and their privileges. A red box highlights the 'User' column.

Username	Server	Action
root	%	Edit
root	127.0.0.1	Edit
9d231610406a		Edit
root	9d231610406a	Edit
root	::1	Edit
localhost		Edit
root	localhost	Edit

En la parte de los usuarios y contraseña logramos ver una contraseña vulnerable la cual fue desencriptada. (root:123456)



The screenshot shows the MySQL 'user' table with the following data:

Host	User	Password	Select_priv
localhost	root	*6BB4837EB74329105EE45680DA7DC67ED2CA2AD9	Y
9d231610406a	root	*6BB4837EB74329105EE45680DA7DC67ED2CA2AD9	Y
127.0.0.1	root	*6BB4837EB74329105EE45680DA7DC67ED2CA2AD9	Y
::1	root	*6BB4837EB74329105EE45680DA7DC67ED2CA2AD9	Y
localhost			N
9d231610406a			N
%	root	*6BB4837EB74329105EE45680DA7DC67ED2CA2AD9	Y

A red box highlights the 'Password' column for the root user, which is '123456'.

CVE-2023-25690

Se establece dicha vulnerabilidad para las versiones desde la 2.4.0 a la 2.4.55 del servidor HTTP apache, donde permite un ataque de contrabando de solicitudes de http.

Existe una configuración en mod_proxy habilitado que permite reescribir una regla o de ProxyPassMatch la cual si adivinamos un patrón que coincide con una parte de los datos destino (URL) proporcionados por el usuario y luego se inserta en el destino de solicitud proxy sustituyendo las variables correspondientes. De esta manera permite la elusión de los controles en los servidores proxy.

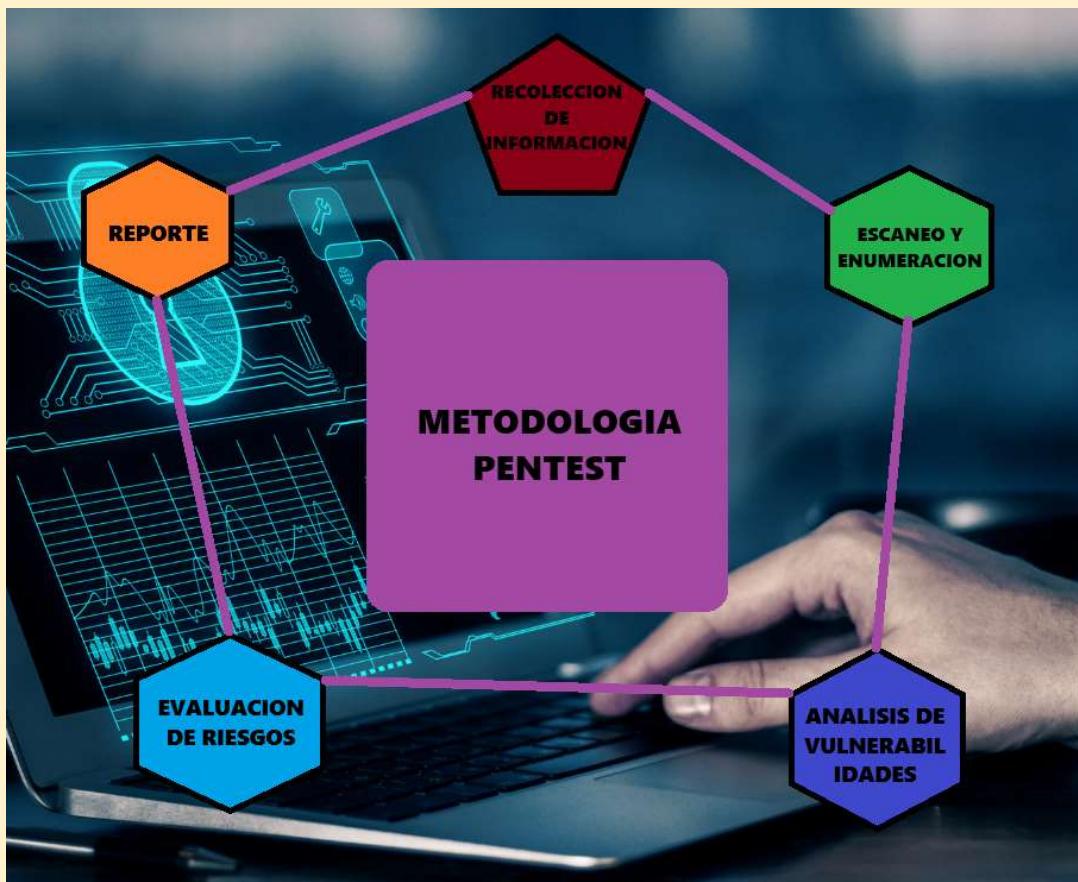
****Recomendaciones:**

- Vulnerabilidad #3: Respecto al servicio HTTP se debe de realizar la busqueda de la version de Apache correspondiente a su ultima actualizacion del servicio e instalar la version mas reciente corrigiendo la misma.
- Utilizacion de Usuarios y contraseñas seguras (12 caracteres con minusculas, mayusculas, numeros y simbolos) con configuracion robusta y no por defecto como administrador o usuario root.
- Utilizacion de llaves SSL garantizando la seguridad, integridad y confidencialidad del cliente.



6) Metodologías.

Un Pentester se sumerge en la mente de un hacker ético, buscando puntos débiles en la seguridad de un sistema antes de que un atacante real pueda explotarlos. Su trabajo es crucial para prevenir violaciones de seguridad y proteger la información confidencial. A través de la prueba de penetración, las organizaciones pueden identificar y corregir vulnerabilidades, mejorar las políticas de seguridad y garantizar la integridad, confidencialidad y disponibilidad de sus activos digitales. Pasos a seguir...



Recolección de Datos:

- Identificar objetivos: Definir claramente el alcance del Pentest y los sistemas a evaluar.
- Obtener información: Recopilar datos sobre la infraestructura, arquitectura de red, aplicaciones y servicios.

Escaneo y Enumeración:

- Escaneo de red: Identificar sistemas activos y servicios en la red.
- Enumeración: Obtener información detallada sobre servicios y usuarios disponibles.

Análisis de Vulnerabilidades:

- Escaneo de vulnerabilidades: Utilizar herramientas para identificar posibles debilidades en sistemas y aplicaciones.
- Ánálisis manual: Investigar vulnerabilidades más allá de las capacidades de las herramientas automáticas.

Evaluación de Riesgos:

- Valoración de amenazas: Determinar el impacto potencial de las vulnerabilidades identificadas.
- Evaluación de riesgos: Clasificar las amenazas según su gravedad y probabilidad de explotación.

Reporte:

- Documentación detallada: Crear un informe que incluya hallazgos, riesgos identificados, evidencia de explotación y recomendaciones.
- Comunicación efectiva: Presentar los resultados de manera comprensible para los equipos de seguridad y la alta dirección.

La prueba de penetración es un proceso continuo y adaptable, ya que las amenazas y tecnologías evolucionan. La colaboración entre Pentesters y equipos de seguridad internos es esencial para mantener la robustez de los sistemas y salvaguardar la información vital en el entorno digital actual.

7) CONCLUSION

La realización de este pentest reveló la existencia de tres vulnerabilidades críticas identificadas como Common Vulnerabilities and Exposures (CVEs).

De estas vulnerabilidades se realizó la demostración y explotación de 2 de ellas, la primera en relación de la enumeración de usuarios, proporcionando nombres de ingreso del sistema si se coloca el diccionario de palabras correspondiente. Luego como segundo caso a explotar vinculada al http-proxy y más específicamente atacando a la base de datos MySQL, se resalta la vulnerabilidad de tráfico web potencial.

Este informe revela la urgencia y prioridad de las prácticas de ciberseguridad y destaca su importancia ante todas las capas de la infraestructura local. Es de gran importancia utilizar e implementar las medidas necesarias de mitigación de riesgos como también de protección de la información confidencial.

Se debe concientizar y capacitar siempre al personal involucrado adoptando mejores prácticas a prevenir futuros accidentes, aplicando las actualizaciones a los sistemas y mantenerse informado o activo a las constantes amenazas cibernéticas que siempre estarán en evolución.