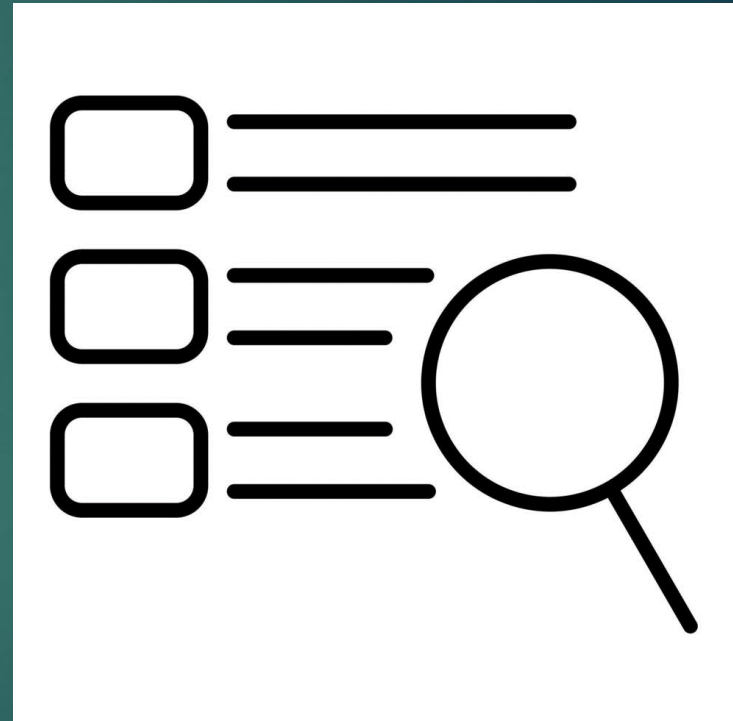


# Informe ejecutivo: Incidente de ciberseguridad en SMART TECH

- ▶ Resumen, Acciones y Recomendaciones

# ÍNDICE

- ▶ Detección de incidente
- ▶ Investigación del incidente
- ▶ Mitigación
- ▶ Hallazgo de una segunda vulnerabilidad
- ▶ Mitigación de una segunda vulnerabilidad
- ▶ Recomendaciones
  - ▶ Creación de plan de recuperación
  - ▶ Topología recomendada
- ▶ Conclusión



# Detección del Incidente

- ▶ Revisión de registros del sistema y servicios críticos
- ▶ Actividad anómala de usuario sin privilegios de administrador



# Investigación del Incidente

- Usuario sin privilegios intentó escalación con sudo (permisos de administrador).

```
Jul 31 16:09:19 debian sudo[1543]:  debian : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl stop speech-dispatcher
Jul 31 16:14:37 debian sudo[1602]:  debian : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/debian ; USER=root ; COMMAND=usermod -aG root debian
Jul 31 16:16:44 debian sudo[1657]:  debian : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/debian ; USER=root ; COMMAND=usermod -aG sudo debian
Jul 31 16:19:16 debian sudo[1684]:  debian : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/sbin/visudo
```

# Investigación del Incidente

- Alteración y eliminación de archivos y procesos del servidor.

```
Oct 08 16:08:57 debian sudo[4687]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install vsftpd
Oct 08 16:09:38 debian sudo[4886]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/vsftpd.con
f
Oct 08 16:10:37 debian sudo[5045]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart vs
ftpd
Oct 08 16:12:13 debian sudo[5104]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install openssh-
server
Oct 08 16:12:55 debian sudo[5157]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/ssh/sshd_c
onfig
Oct 08 16:14:16 debian sudo[5335]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart ss
h
Oct 08 16:16:37 debian sudo[5480]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/ls -l /var/www/html
Oct 08 16:17:59 debian sudo[5532]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/chmod -R 777 /var/ww
w/html
Oct 08 16:20:04 debian sudo[5592]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/chmod 777 /var/www/h
tml/wp-config.php
Oct 08 16:21:23 debian sudo[5646]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/apache2/ap
ache2.conf
Oct 08 16:24:30 debian sudo[5975]:  debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart ap
```

# Mitigación

- ▶ Eliminación de usuario 'wordpressuser'
- ▶ Refuerzo de contraseñas de usuario root y wordpress
- ▶ Desactivación de acceso anónimo en FTP
- ▶ Migración a autenticación por llave SSH y bloqueo de root
- ▶ Actualización completa de sistema y parches



```
debian@debian:/var/www/html$ sudo su
root@debian:/var/www/html# passwd
New password:
Retype new password:
passwd: password updated successfully
root@debian:/var/www/html#
```

```
MariaDB [(none)]> SELECT User , Host FROM mysql.user;
+-----+-----+
| User      | Host      |
+-----+-----+
| mariadb.sys | localhost |
| mysql      | localhost |
| root       | localhost |
| user       | localhost |
| wordpressuser | localhost |
+-----+-----+
5 rows in set (0.026 sec)

MariaDB [(none)]> DROP USER 'wordpressuser'@'localhost';
Query OK, 0 rows affected (0.079 sec)

MariaDB [(none)]> SELECT User, Host FROM mysql.user WHERE User = 'wordpressuser';
Empty set (0.006 sec)
```



# Hallazgo de una segunda vulnerabilidad

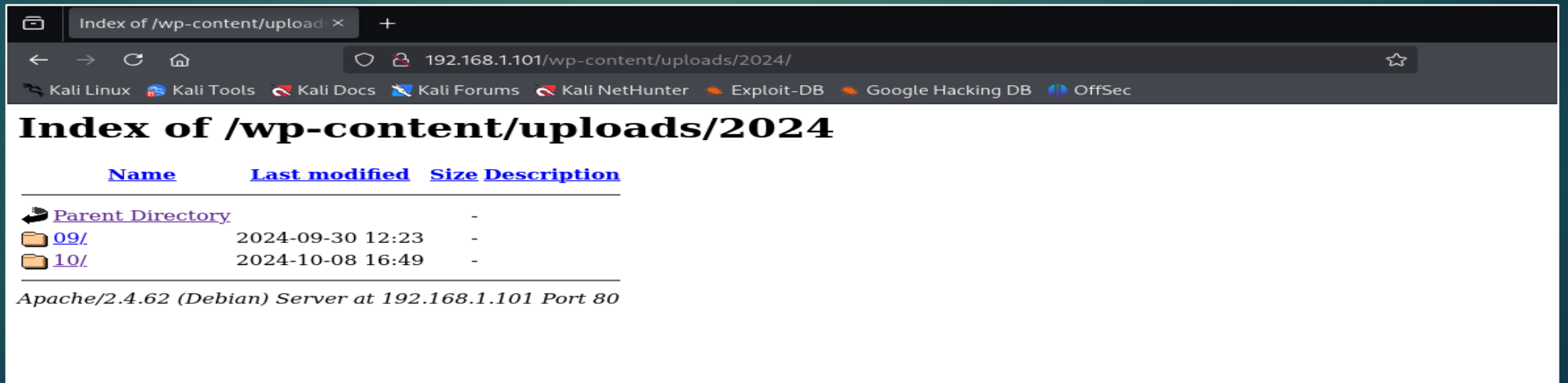
## ► Pentesting y hallazgo de vulnerabilidad

```
80/tcp open  http      Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-phpmyadmin-dir-traversal:
|   VULNERABLE: phpMyAdmin versions 2.6.4 and 2.6.4-pl1.
|   phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
|   State: LIKELY VULNERABLE
|   IDs: CVE:CVE-2005-3299
|   PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1 allows r
emote attackers to include local files via the $__redirect parameter, possibly involving the subform array.
|
|   Disclosure date: 2005-10-nil
|   Extra information:
|   ../..../..../..../etc/passwd not found.
|
|   References: Assigned CVE id: CVE-2005-3299
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
|   http://www.exploit-db.com/exploits/1244/
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /readme.html: Wordpress version: 2
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /readme.html: Interesting, a readme.
MAC Address: 08:00:27:99:E6:A9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.82 seconds
```

# Hallazgo de una segunda vulnerabilidad

- ▶ Indexación de directorios web.
  - ▶ Exposición de archivos internos del servidor



The screenshot shows a web browser window with the address bar displaying `192.168.1.101/wp-content/uploads/2024/`. The browser's bookmark bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area displays the title "Index of /wp-content/uploads/2024" and a table with the following columns: Name, Last modified, Size, and Description. The table lists a "Parent Directory" link and two subdirectories, "09/" and "10/". At the bottom, a footer indicates the server is "Apache/2.4.62 (Debian) Server at 192.168.1.101 Port 80".

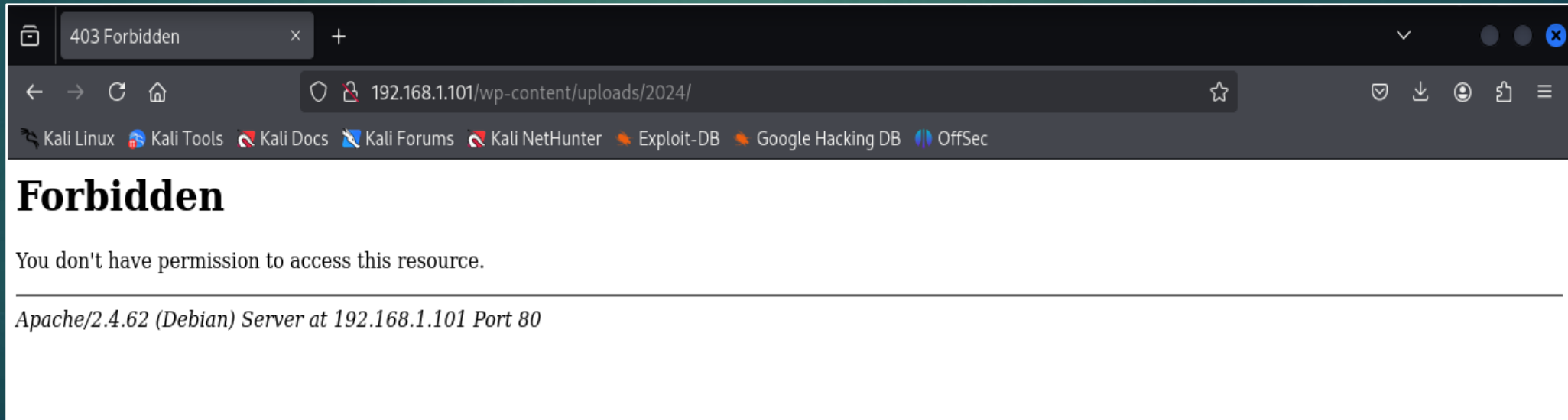
Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">09/</a>	2024-09-30 12:23	-	-
<a href="#">10/</a>	2024-10-08 16:49	-	-

Apache/2.4.62 (Debian) Server at 192.168.1.101 Port 80



# Mitigación de una segunda vulnerabilidad

- ▶ Modificación de archivo de configuración de apache
- ▶ Reinicio de servicio de apache



# Recomendaciones



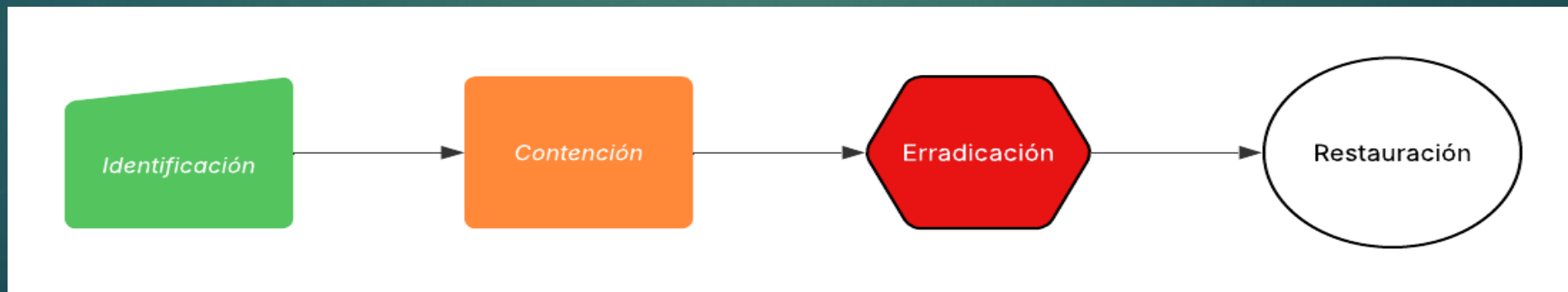
# Recomendaciones

Se debe:

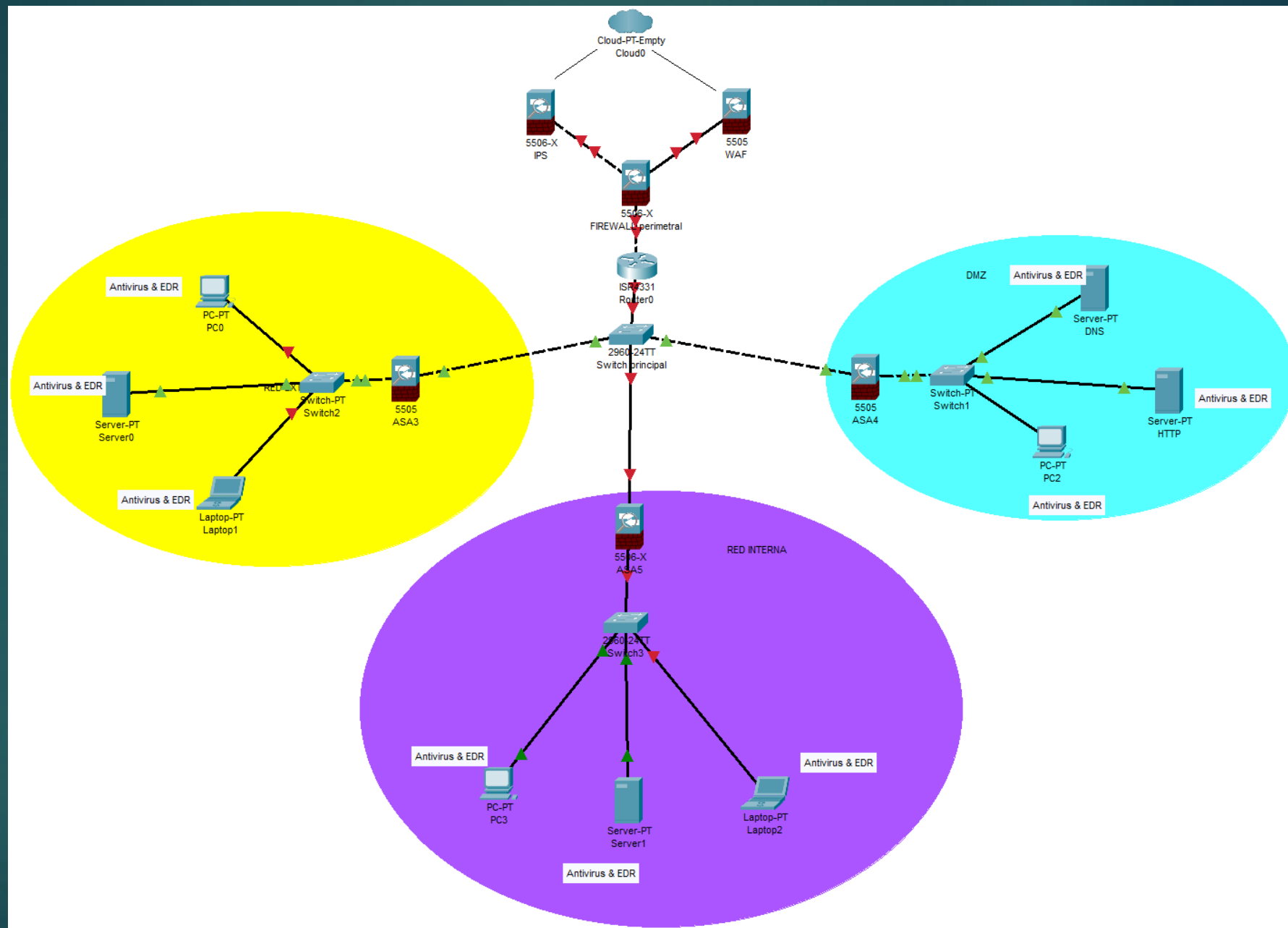
- ▶ Implementar políticas de contraseñas robustas y rotación periódica
- ▶ Activar el plugin “validate\_password” en MySQL para forzar contraseñas seguras
- ▶ Deshabilitar contraseñas SSH y usar llaves públicas
- ▶ Auditar configuraciones críticas regularmente
- ▶ Deploy fail2ban y WAF para protección adicional
- ▶ Capacitación continua del personal y simulacros de incidente
- ▶ Mitigar las demás vulnerabilidades no abordadas en este informe, pero si presentes en el servidor.
- ▶ Evitar subir archivos confidenciales (backups, archivos de configuración) al directorio web público
- ▶ Establecer respaldos automáticos y almacenarlos fuera del servidor.

# Creación de plan de recuperación

- ▶ Identificación: Logs, actividades anómalas, clasificación del incidente
- ▶ Contención: Aislamiento, bloqueo de accesos y obtención de evidencia
- ▶ Erradicación: Limpieza de malware y revocación de credenciales
- ▶ Restauración: Recuperación desde respaldos limpios y validación de integración y funcionalidad



# Topología recomendada





## 5. Conclusión

- El incidente evidenció debilidades en la configuración y hábitos de seguridad. Las acciones aplicadas mitigaron el riesgo actual y establecieron las bases para una postura de seguridad proactiva, pero sigue siendo necesario tomar un rol activo, realizar las actividades recomendadas y darle una importancia más alta a la ciberseguridad con el objetivo de evitar futuros ataques al anticipar y corregir vulnerabilidad por medio de revisiones constantes.