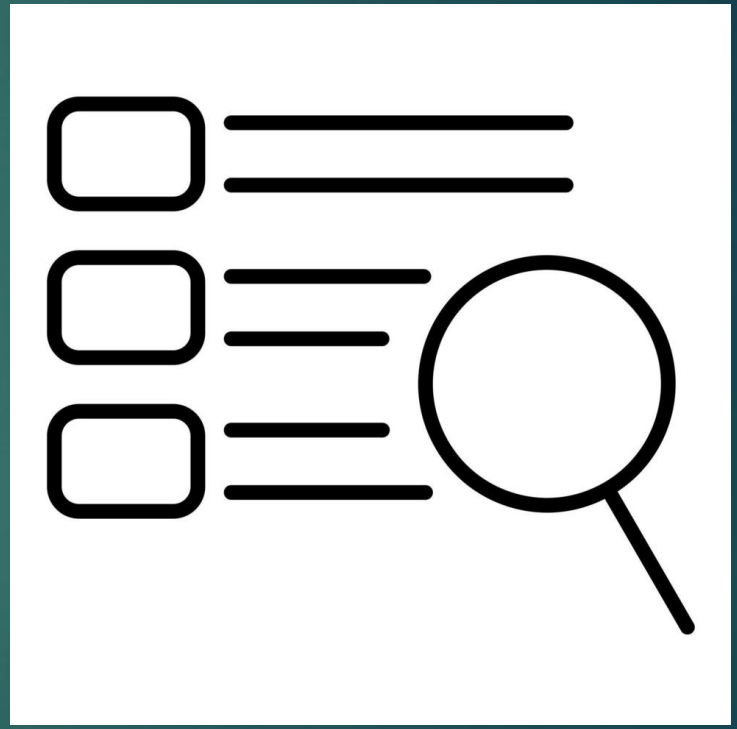
Informe ejecutivo: Incidente de ciberseguridad en SMART TECH

- Resumen, Acciones y Recomendaciones

Proyecto Final / Alan Alvarado – Junio 2025

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).
- Alteración y eliminación de archivos y procesos del servidor.

```
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=userm
ood -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=userm
ood -aG sudo debian
```

```
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#
```

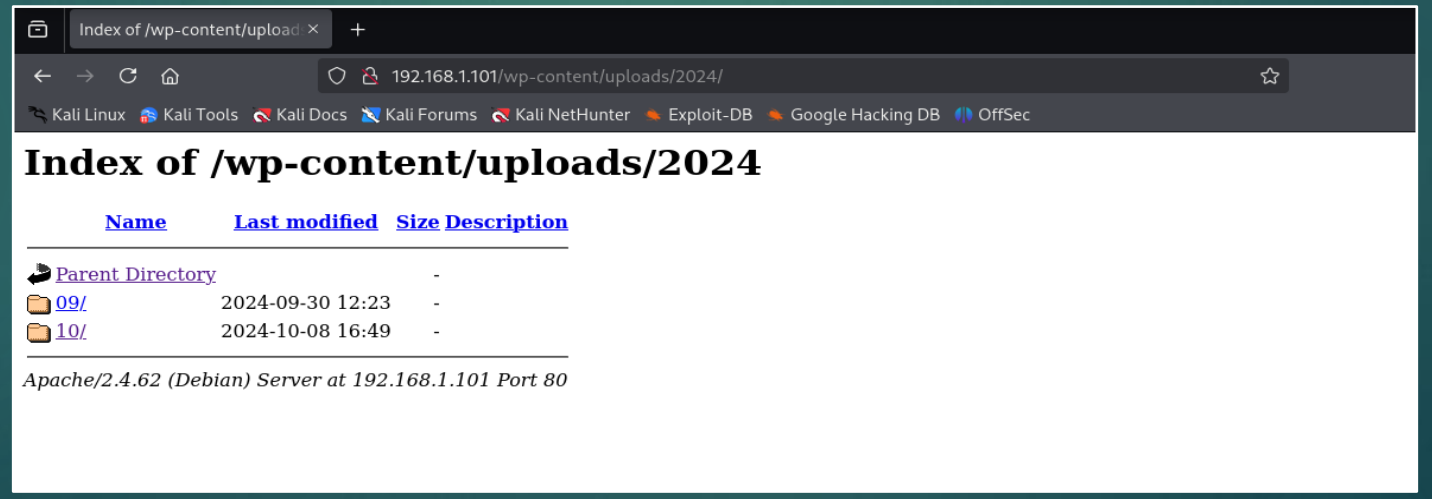
```
MariaDB [(none)]> SELECT User , Host FROM mysql.user;
+---------------+-----------+
| User          | Host      |
+---------------+-----------+
| mariadb.sys   | localhost |
| mysql         | localhost |
| root          | localhost |
| user          | localhost |
| wordpressuser | localhost |
+---------------+-----------+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

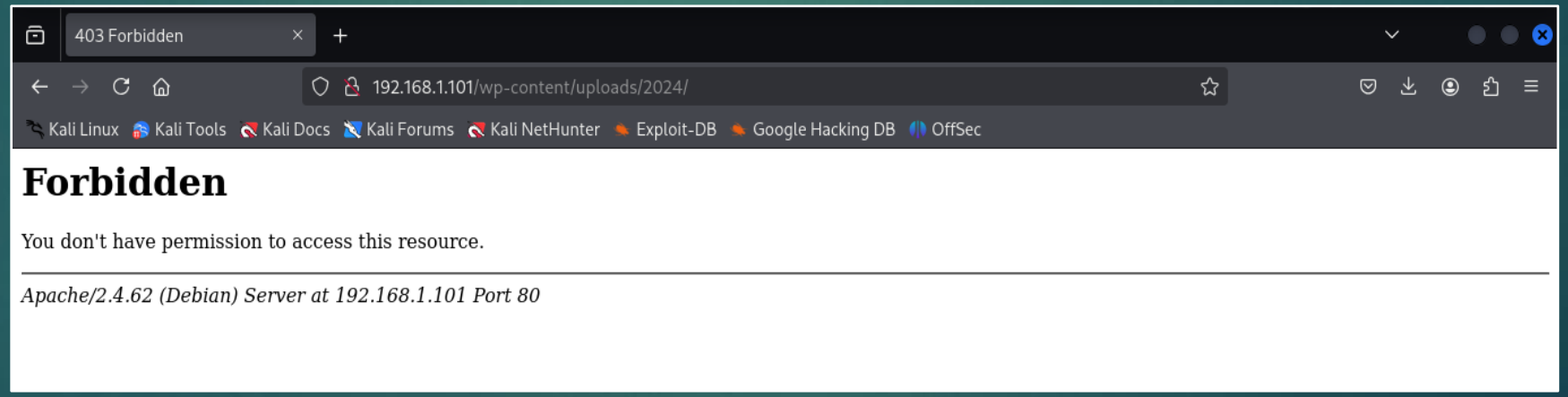
Hallazgo de una segunda vulnerabilidad

- Pentesting y hallazgo de vulnerabilidad
- Indexación de directorios web.
  - Exposición de archivos internos del servidor



Mitigación de una segunda vulnerabilidad

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



Recomendaciones

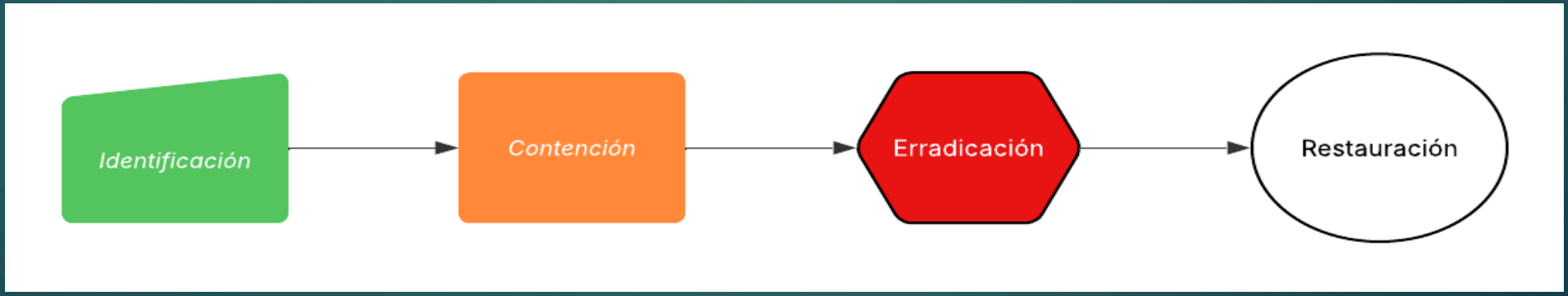
Recomendaciones

Se debe:

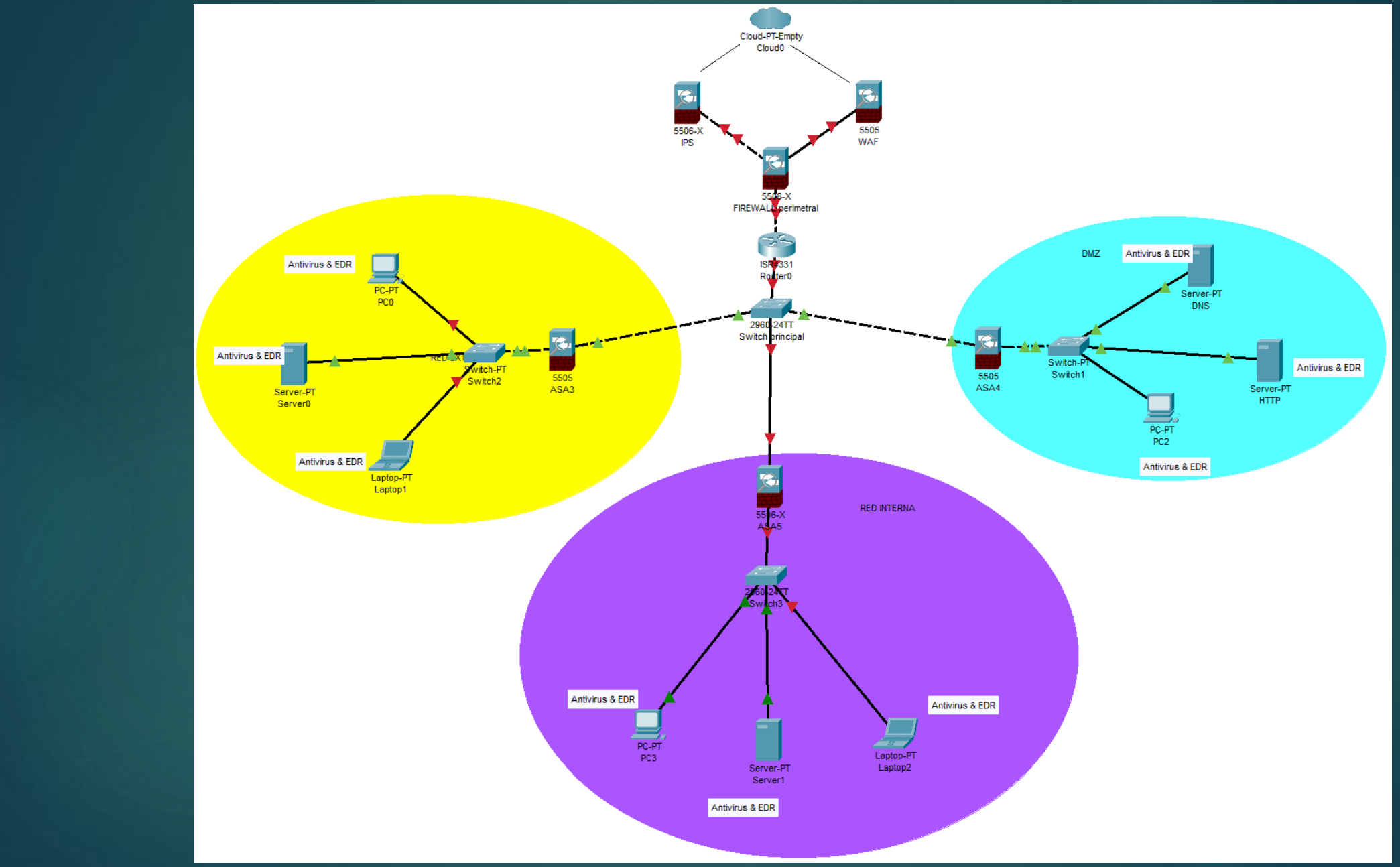
- Implementar políticas de contraseñas robustas y rotación periódica
- Activar el plugin “validate_password” en MySQL para forzar contraseñas seguras
- Deshabilitar contraseñas SSH y usar llaves públicas
- Auditar configuraciones críticas regularmente
- Deploy fail2ban y WAF para protección adicional
- 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


Cloud-PT-Empty
Cloud0
5506-X
IPS
5505
WAF
5506-X
FIREWALL perimetral
ISR4331
Router0
2960-24TT
Switch principal
Antivirus & EDR
PC-PT
PC0
Antivirus & EDR
Server-PT
Server0
Switch-PT
Switch2
5505
ASA3
Antivirus & EDR
Laptop-PT
Laptop1
DMZ
Antivirus & EDR
Server-PT
DNS
5505
ASA4
Switch-PT
Switch1
Server-PT
HTTP
Antivirus & EDR
PC-PT
PC2
Antivirus & EDR
RED INTERNA
5506-X
ASA5
2960-24TT
Switch3
Antivirus & EDR
PC-PT
PC3
Server-PT
Server1
Laptop-PT
Laptop2
Antivirus & EDR
Antivirus & EDR

5. Conclusión

- El incidente evidenció debilidades en la configuración y hábitos de seguridad. Las acciones aplicadas mitigaron el riesgo actual y establecieron bases sólidas 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.