

INFORME DE AUDITORÍA INFORMÁTICA

QuickPrint Soluciones S.L.

CiberSecure Consultores S.L.

Gracia, Lorena y Cristóbal

27 de octubre – 31 de octubre de 2025

Página de Presentación

Este informe recoge los resultados de la auditoría informática realizada a QuickPrint Soluciones

S.L. por CiberSecure Consultores S.L., entre el 27 y el 31 de octubre de 2025, siguiendo las

directrices del RGPD, LOPDGDD e ISO 27001. El objetivo fue evaluar el nivel de seguridad y

cumplimiento normativo del sistema informático de la entidad.

[**Informe de Auditoría del Sistema Informático de QuickPrint Soluciones S.L. 5**](#_gjdgxs)

[1. Resumen Ejecutivo 5](#_30j0zll)

[2. Identificación del Cliente / Entidad Auditada 5](#_1fob9te)

[3. Objetivos de la Auditoría 5](#_3znysh7)

[4. Normativas y Referenciales Aplicados 6](#_2et92p0)

[5. Alcance de la Auditoría 6](#_tyjcwt)

[6. Metodología de Auditoría 6](#_3dy6vkm)

[7. Contexto del Sistema Auditado 7](#_1t3h5sf)

[8. Cumplimiento Normativo 10](#_4d34og8)

[9. Riesgos y Hallazgos de Seguridad 10](#_2s8eyo1)

[9.1. Riesgos críticos 10](#_17dp8vu)

[9.2. Hallazgos adicionales 11](#_3rdcrjn)

[10. Fortalezas (Hardening) 11](#_26in1rg)

[11. No Conformidades 12](#_lnxbz9)

[12. Recomendaciones 12](#_35nkun2)

[1. Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) 12](#_1ksv4uv)

[2. Actualizar Software Crítico y Sistema Operativo 12](#_44sinio)

[3. Configurar y Activar Firewall, IDS/IPS y WAF 13](#_2jxsxqh)

[4. Políticas de Contraseñas y Control de Accesos 13](#_z337ya)

[5. Migrar la Red Wi-Fi a WPA2/WPA3 con Radius y Desactivar WPS 14](#_3j2qqm3)

[6. Desactivar Servicios No Esenciales 14](#_1y810tw)

[7. Cifrar Bases de Datos y Comunicaciones Web 15](#_4i7ojhp)

[8. Implementar Headers de Seguridad Web 15](#_2xcytpi)

[9. Formación en Ciberseguridad y Concienciación 16](#_1ci93xb)

[10. Copias de Seguridad Automáticas y Cifradas 16](#_3whwml4)

[11. Formar al Personal en Ciberseguridad 17](#_2bn6wsx)

[13. Conclusiones 17](#_qsh70q)

[14. Anexos 18](#_3as4poj)

[ANEXO 1 - PRESUPUESTO DE LAS RECOMENDACIONES 19](#_1pxezwc)

[ANEXO 2 - CAPTURAS Y EVIDENCIAS TÉCNICAS 21](#_49x2ik5)

[ANEXO 3 - DIAGRAMA DE RED (TOPOLOGÍA DE RED ACTUAL) 40](#_2p2csry)

[ANEXO 4 - TABLA DE EVIDENCIAS 41](#_147n2zr)

[ANEXO 5 - LISTADO DE SOFTWARE Y VERSIONES DETECTADAS 41](#_3o7alnk)

# 

# 

# 

# 

# 

# **Informe de Auditoría del Sistema Informático de QuickPrint Soluciones S.L.**

Fecha de realización: 27/10/2025 - 03/11/2025

Versión del informe: 3.0

Equipo Auditor: Cristobal, Gracia y Lorena

Entidad auditora: CiberSecure Consultores S.L.

## **1. Resumen Ejecutivo**

El presente informe recoge los resultados de la auditoría informática realizada a **QuickPrint Soluciones S.L.**, con el objetivo de evaluar el nivel de cumplimiento normativo (especialmente **RGPD/LOPDGDD**) y la seguridad de los sistemas informáticos.

Durante la auditoría se detectaron **debilidades significativas** en la configuración, gestión y protección de los sistemas, destacando la presencia de **software obsoleto**, la **ausencia de cifrado (TLS)** en las comunicaciones web y la exposición de servicios críticos (SSH y FTP) con **controles de acceso deficientes** (contraseñas débiles). Esto implica un **incumplimiento grave** de las normativas de protección de datos personales.

El informe detalla las vulnerabilidades encontradas, el impacto potencial sobre la organización y las medidas correctoras recomendadas para garantizar el cumplimiento de las normativas vigentes (LOPDGDD, RGPD, ISO 27001, ENS, etc.) y garantizar un nivel de seguridad aceptable.

## **2. Identificación del Cliente / Entidad Auditada**

* **Cliente/Entidad Auditada:** **QuickPrint Soluciones S.L.** (Imprenta digital y soluciones de gestión documental).

## **3. Objetivos de la Auditoría**

El objetivo general fue realizar un ejercicio completo de seguridad en equipo que incluyó:

* Reconocimiento y enumeración de la red, análisis de tráfico y paquetes.
* Auditoría de servicios, análisis de logs y control de accesos.
* Detección de vulnerabilidades y configuraciones inseguras en sistemas y aplicaciones.
* Propuesta de medidas de protección (firewall, endurecimiento).
* Generar un informe final con hallazgos, medidas de remediación y cumplimiento normativo.

BENEFICIOS TANGIBLES

* Reducción 90% riesgo ciberataques
* Cumplimiento ISO 27001 básico
* Recuperación garantizada ante incidentes
* Mejora productividad y confianza clientes

## **4. Normativas y Referenciales Aplicados**

Los referenciales utilizados para la auditoría y las recomendaciones incluyen:

* **PROTECCIÓN DE DATOS (Esencial):**
* Reglamento General de Protección de Datos (RGPD) + Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
* **COMERCIO ELECTRÓNICO:**
* Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) y Ley General para la Defensa de los Consumidores y Usuarios.
* **SEGURIDAD INFORMÁTICA (Recomendado):**
* Esquema Nacional de Seguridad (ENS) e ISO 27001.

## **5. Alcance de la Auditoría**

La auditoría se centró en los principales activos de la red local, incluyendo el mapeo y análisis de los siguientes dispositivos y servicios, con el objetivo de generar un informe con hallazgos y medidas de remediación:

* **Activos Principales:** Router principal, Servidor principal (Web/FTP/BBDD), PCs de trabajo (Linux), Impresoras con WiFi, Puntos de acceso WiFi.
* **Segmento de Red (IP):** 192.168.0.0/24.
* **Hosts analizados:** 192.168.0.21, 192.168.0.43, 192.168.0.58, entre otros.
* **Servicios Críticos Analizados:** SSH (Puerto 22), HTTP (Puerto 80), FTP.
* **Alcance Lógico:** Red inalámbrica, Red local, Servidor Principal, PC de trabajo, Impresoras/Dispositivos IoT, y políticas de acceso/usuarios.

Duración: 7 días hábiles.

## **6. Metodología de Auditoría**

Se utilizó una metodología mixta basada en análisis técnico, entrevistas y observación directa, siguiendo las directrices de la norma ISO 19011 para auditorías.

**6.1. Técnicas utilizadas:**

Se aplicó una metodología de *pentesting* y auditoría técnica basada en el sistema operativo Kali.

|  |  |  |
| --- | --- | --- |
| **Fase** | **Objetivo** | **Herramientas Clave** |
| **Reconocimiento y mapeo** | Identificar hosts activos, puertos y servicios. | arp-scan, netdiscover, Nmap. |
| **Análisis de tráfico** | Capturar tráfico relevante y analizar patrones/anomalías. | tcpdump, Wireshark, tshark. |
| **Auditoría de Vulnerabilidades** | Verificar configuraciones y debilidades. | Nmap scripts, Nikto, whatweb. |
| **Control de Accesos/Passwords** | Auditar cuentas de usuario y políticas. | Nmap + Hydra (Fuerza bruta sobre SSH). |
| **Enumeración de servicios** | Verificar configuraciones visibles y vulnerabilidades. | Nmap scripts (--script=vuln), curl, Nikto, whatweb. |
| **Análisis de Logs** | Revisar logs del sistema/servicios para identificar actividad sospechosa | grep, journalctl, ausearch. |
| **Gestión de Usuarios/Permisos** | Demostrar creación de cuentas, grupos y auditar permisos. | adduser, groupadd, usermod, chown, chmod. |
| **Hardening/Remediación** | Aplicar medidas de protección. | nftables (Firewall), fail2ban (Protección contra fuerza bruta). |

## **7. Contexto del Sistema Auditado**

**7.1.1 Descripción de la organización**

**QuickPrint Soluciones S.L.** es una copistería digital y empresa de diseño gráfico con operaciones locales y online. Opera con un sistema informático que soporta la gestión de impresión, la base de datos de clientes y los servicios web para recibir pedidos. Los procesos clave implican el manejo de datos personales y la transferencia de documentos (vía FTP y red local).

**7.1.2 Procesos principales**

• Recepción de archivos de impresión (presencial y vía web).

• Procesamiento y maquetación digital.

• Facturación y gestión de clientes.

• Comunicación con clientes vía web y móvil.

**7.2. Estructura de la Entidad Auditada: QuickPrint Soluciones S.L.**

**Nombre y Datos de la Entidad**

* **Nombre de la Imprenta Auditada:** **QuickPrint Soluciones S.L.**
* **Sector:** Impresión digital y soluciones de gestión documental, con alto manejo de datos de clientes a través de su plataforma web.
* **Contexto de la Auditoría:** Evaluación del SGSI, seguridad de red y cumplimiento del **RGPD y la LOPDGDD** debido al manejo de información personal de clientes.

**Estructura Organizativa y Roles Internos**

El ecosistema de red incluye:

* **Router principal:** Conecta a Internet y a la red local.
* **Aplicaciones web en WordPress** (versión desactualizada).
* **Servidor principal:** Gestión de impresión, FTP, base de datos de clientes, web.
  + **Software detectado:** Apache httpd 2.4.65 (Debian) , OpenSSH 10.0p2 Debian 8.
* **PC de trabajo (Linux):** Impresiones, administración, envíos.
* **Dispositivos de Impresión:** Impresoras con WiFi (reciben documentos desde PC y móviles).
* **Red Inalámbrica:** Puntos de acceso WiFi, móviles personales de empleados (uso laboral).
* **Dispositivo WiFi desconocido:** Dispositivo conectado, posible intruso.

Para relacionar los hallazgos técnicos del informe (IPs y ataques demostrados) con el personal interno:

|  |  |  |
| --- | --- | --- |
| **Rol Clave** | **Tareas Principales (En el contexto de la red)** | **Activo Informático Clave** |
| **Director de Administración/Sistemas**  ( Antonio) | Gestión de pedidos, facturación, manejo de datos sensibles, acceso remoto seguro (SSH). | **PC de Trabajo (Linux) - IP \*.21** (PC atacado con fuerza bruta por tener **contraseña débil**). |
| **Diseño y Preimpresión** (Marta) | Procesamiento de archivos de clientes, interacción con Servidor FTP. | **PC/Workstation - IP \*.58** (PC utilizado como **equipo puente** en el ejercicio de *Hardening EXTRA*). |
| **Técnico de Infraestructura** (Javier) | Mantenimiento físico y lógico del Servidor Principal y gestión de la red. | **Servidor Principal - IP \*.50** |

#### 

**Estructura de la Red y Activos Informáticos**

La topología de red corresponde a una red local tradicional con exposición pública en el servidor web.

|  |  |  |  |
| --- | --- | --- | --- |
| **Activo (Dispositivo)** | **Dirección IP Clave (Referencia)** | **Servicios y Función Principal** | **Hallazgo de Seguridad Relevante** |
| **Servidor Principal** | 192.168.0.50 (o similar) | Alojamiento Web (Apache), FTP, Base de Datos. | **FTP Anónimo activo, Software Obsoleto, Ausencia de TLS (HTTP)**. |
| **PC de Administración** | 192.168.0.21 | Terminal Linux, SSH expuesto. | **Contraseña débil** (probado con *Nmap + Hydra*). |
| **Router Principal** | 192.168.0.1 | Gateway, conecta a Internet. | Falta de configuración de Firewall. |
| **Puntos de Acceso WiFi** | N/A | Conectividad para impresoras y móviles de empleados. | **WPS Activo, WPA débil** (riesgo de *sniffing*). |
| **Dispositivo Desconocido** | 192.168.0.99 | Conexión de origen no identificado. | **Riesgo crítico de intrusión**. |

## 

## **8. Cumplimiento Normativo**

Se observa un incumplimiento grave en normativas clave:

* **RGPD y LOPDGDD:** Incumplimiento por falta de cifrado (TLS/SSL), control de accesos inadecuado y ausencia de documentación clave (Registro de Actividades, Protocolo de Incidentes).
* **Seguridad de la Información (ENS/ISO 27001):** Inmadurez en la gestión, falta de implementación proactiva de herramientas de protección (IDS/IPS/WAF) y ausencia de un SGSI básico.

## **9. Riesgos y Hallazgos de Seguridad**

El análisis de vulnerabilidades (Nikto, Nmap, Whatweb) reveló hallazgos significativos.

### **9.1. Riesgos críticos**

**Prioridad ALTA**

|  |  |  |
| --- | --- | --- |
| **Evidencia** | **Riesgo / Impacto** | **Recomendación Inmediata** |
| **SSH expuesto con contraseña débil** (en PC \*.21). | **Alto:** Acceso remoto y escalada de privilegios. | Cambiar a clave SSH (RSA) y establecer **Autenticación de 2 Factores (2FA)**. |
| **Software de Servidor Desactualizado**. | **Alto:** Explotación de vulnerabilidades conocidas (CVE). | **Actualizar todo el software** de forma inmediata y aplicar gestión de parches. |
| **Falla TLS (sin HTTPS)** | **Alto:** Transmisión de datos sensibles y credenciales sin cifrado. | Habilitar TLS/SSL en el servidor web (Puerto 443). |
| **FTP Anónimo activo** | **Alto:** Acceso no autorizado a documentos/archivos. | Deshabilitar el acceso FTP anónimo. |
| **Red Wi-Fi WEP/WPA débil o WPS activo**. | **Muy Alto:** Intrusión a toda la red, *sniffing* de tráfico. | Migrar a **WPA2/WPA3**, y **desactivar WPS**. |

### 

### **9.2. Hallazgos adicionales**

**Prioridad MEDIA/BAJA**

|  |  |  |
| --- | --- | --- |
| **Evidencia** | **Riesgo / Impacto** | **Mitigación Técnica** |
| Falta X-Content-Type-Options. | **Media:** Permite a navegadores ejecutar código malicioso por *MIME sniffing*. | Añadir el *header* X-Content-Type-Options: nosniff. |
| Falta X-Frame-Options. | **Baja:** Facilita ataques de *clickjacking*. | Añadir X-Frame-Options: SAMEORIGIN o DENY. |
| Software de impresión con exposición de red interna. | **Media:** Posible manipulación de documentos. | Conectar sólo a red interna segmentada. |

## 

## **10. Fortalezas (Hardening)**

El equipo auditor demostró la capacidad de aplicar medidas de endurecimiento (*Hardening*):

1. **Configuración de Firewall:** Implementación de un **firewall con nftables** para filtrar el tráfico de entrada.
2. **Protección de autenticación:** Instalación y configuración de **fail2ban** para detener intentos de autenticación no autorizados (fuerza bruta SSH).
   * **Nota:** Se observó que un servicio mal configurado puede usarse para enmascarar un ataque, ya que la IP del PC de Diseño (\*.58) fue baneada al lanzar el ataque (simulado por Javier desde \*.43) contra el PC de Administración (\*.21).

## 

## **11. No Conformidades**

La auditoría revela las siguientes no conformidades que suponen graves deficiencias:

* Gestión inmadura de la seguridad (ausencia de SGSI).
* Falta de gestión de parches/vulnerabilidades en el software.
* Ausencia de firewall, IDS/IPS o WAF bien configurados en la infraestructura.
* Falta de registro de incidentes y accesos.
* Incumplimiento del RGPD y LOPDGDD.
* Contraseñas compartidas y sin política de caducidad.

## **12. Recomendaciones**

Se establecen las siguientes recomendaciones, priorizando la seguridad y el cumplimiento normativo:

#### **1. Implementar un Sistema de Gestión de Seguridad de la Información (SGSI)**

**Objetivo:** Establecer políticas, procedimientos y controles basados en la norma **ISO 27001**.  
 **Acciones:**

* Designar un **Responsable de Seguridad de la Información (RSI)** interno.
* Elaborar los documentos mínimos: *Política de Seguridad, Análisis de Riesgos, Plan de Continuidad, Plan de Copias de Seguridad, Protocolo de Incidentes y Registro de Actividades de Tratamiento (RGPD)*.
* Utilizar plantillas o software SGSI (por ejemplo: *ISOTools, Open-AudIT, o Microsoft Purview Compliance Manager*).
* Realizar revisiones trimestrales de seguridad.

**Prioridad:** Alta  
**Responsable:** Dirección + Técnico de Infraestructura

#### **2. Actualizar Software Crítico y Sistema Operativo**

**Objetivo:** Corregir vulnerabilidades conocidas (CVE) y eliminar software obsoleto.  
 **Acciones:**

Ejecutar actualizaciones del sistema Debian con:  
 sudo apt update && sudo apt upgrade -y

* Actualizar Apache, OpenSSH, PHP y CMS (WordPress) a sus últimas versiones estables todos los plugins/temas.

**Prioridad:** Crítica  
**Responsable:** Técnico de Infraestructura

#### 

#### **3. Configurar y Activar Firewall, IDS/IPS y WAF**

**Objetivo:** Filtrar tráfico malicioso y prevenir accesos no autorizados.  
 **Acciones:**

Implementar **nftables** con reglas básicas de denegación por defecto:  
 nft add rule inet filter input ct state established,related accept

nft add rule inet filter input tcp dport {22,80,443} accept

nft add rule inet filter input drop

* Instalar **Fail2Ban** para bloquear intentos de fuerza bruta.
* Instalar un **IDS/IPS** como *Suricata*.
* Implementar un **WAF** (Web Application Firewall) con *ModSecurity* sobre Apache.
* Registrar logs y alertas en un sistema central (ej.ELK, Grafana).

**Prioridad:** Alta  
**Responsable:** Técnico de Infraestructura + Consultor externo (si procede)

#### 

#### **4. Políticas de Contraseñas y Control de Accesos**

**Objetivo:** Prevenir accesos indebidos y contraseñas débiles.  
 **Acciones:**

* No utilizar para las conexiones al sistema los usuarios que vienen por defecto (‘root’), ni las claves que vengan por defecto. Crear un nuevo usuario administrador para Linux, así como los necesarios para cada puesto y cada empleado.
* Crear cuentas nombradas con permisos mínimos necesarios
* Definir una **política de contraseñas** (mínimo 12 caracteres, con complejidad).
* Activar caducidad cada 90 días (chage en Linux).
* Deshabilitar usuarios inactivos y genéricos
* Deshabilitar usuarios de personal que ya no trabaja en la empresa
* Implementar **autenticación por clave SSH RSA (2048 bits o superior)**.
* Activar **2FA (Two-Factor Authentication)** en accesos críticos (ej. SSH, WordPress, paneles administrativos).

**Prioridad:** Alta  
 **Responsable:** Administración de Sistemas

#### **5. Migrar la Red Wi-Fi a WPA2/WPA3 con Radius y Desactivar WPS**

**Objetivo:** Aumentar la seguridad de la red inalámbrica y evitar intrusiones.  
 **Acciones:**

* Desactivar WPS desde la interfaz del router y ocultar SSID.
* Configurar autenticación WPA2/WPA3-Enterprise con **FreeRADIUS** o **Windows NPS**.
* Crear VLAN o SSID separados para invitados y dispositivos IoT.
* Servidor web/FTP (en DMZ)
* Registrar y controlar los MAC autorizados.

**Prioridad:** Alta  
 **Responsable:** Técnico de Infraestructura

#### 

#### **6. Desactivar Servicios No Esenciales**

**Objetivo:** Reducir la superficie de ataque.  
 **Acciones:**

* Deshabilitar FTP anónimo en /etc/vsftpd.conf (anonymous\_enable=NO).
* Migrar a **SFTP o FTPS** (seguro).

Eliminar servicios innecesarios con:  
 systemctl disable nombre\_servicio

* Revisar puertos abiertos (nmap o netstat) y cerrar los no utilizados.

**Prioridad:** Alta  
**Responsable:** Técnico de Infraestructura

#### **7. Cifrar Bases de Datos y Comunicaciones Web**

**Objetivo:** Proteger datos personales y credenciales.  
 **Acciones:**

* Automatizar backups diarios de:

– Base de datos

– Archivos de WordPress y configuraciones del servidor

– Documentos críticos del negocio

* Instalar certificado **TLS (Let’s Encrypt o SSL comercial)**:  
  sudo certbot --apache
* Forzar redirección HTTPS (rewrite en Apache).
* Activar cifrado de base de datos (en MySQL con AES\_ENCRYPT o capa de disco LUKS).
* Probar configuración con ssllabs.com/ssltest.

**Prioridad:** Crítica  
**Responsable:** Técnico de Infraestructura

#### **8. Implementar Headers de Seguridad Web**

**Objetivo:** Proteger contra ataques web comunes (clickjacking, MIME sniffing, etc.).  
 **Acciones:**

Añadir en /etc/apache2/conf-enabled/security.conf:  
Header always set X-Frame-Options "SAMEORIGIN"

Header always set X-Content-Type-Options "nosniff"

Header always set X-XSS-Protection "1; mode=block"

* Verificar con securityheaders.com.

**Prioridad:** Media  
**Responsable:** Técnico Web

#### **9. Formación en Ciberseguridad y Concienciación**

**Objetivo:** Reducir el riesgo humano (phishing, contraseñas débiles, mal uso de datos).  
 **Acciones:**

* Impartir **formación trimestral** al personal sobre:
  + Phishing y ingeniería social.
  + Protección de datos (RGPD/LOPDGDD).
  + Uso seguro de dispositivos personales (BYOD).
* Utilizar plataformas de formación como *INCIBE, CSIRT-CV o AwarenessHub*.

**Prioridad:** Media  
**Responsable:** Dirección y Gestión de RHH

#### **10. Copias de Seguridad Automáticas y Cifradas**

**Objetivo:** Garantizar la continuidad del negocio.  
 **Acciones:**

* Implementar **copias automáticas** diarias con *rsync + cron* o herramientas tipo *BorgBackup*.
* Cifrar los respaldos con gpg o duplicity.
* Mantener una copia **offline o en la nube segura (S3, Azure Backup)**.
* Verificar restauración trimestralmente.

**Prioridad:** Alta  
**Responsable:** Técnico de Infraestructura

#### **11. Formar al Personal en Ciberseguridad**

* Realizar talleres trimestrales sobre:

– Phishing y fraudes digitales

– Manejo de contraseñas y evidencias

– Uso seguro de dispositivos personales

– Políticas de respaldo y confidencialidad

**Objetivo:** reducir riesgo humano, principal vector de ataque.

**12. Monitorización continua y auditorías periódicas**

* Implementar sistema de monitoreo de logs y alertas (Zabbix, ELK).
* Revisar mensualmente los registros del servidor, WAF y firewall.
* Programar auditorías externas trimestralmente (o máximo cada seis meses).

**Objetivo:** detección temprana y mejora continua.

**13. Opcionales / Complementarios**

* Implementar control de dispositivos USB y cifrado de discos (BitLocker o

LUKS).

* Establecer política de retención y borrado seguro de datos (eliminación de archivos temporales, y/o documentos generados por la actividad diaria, con programación diaria y mensual).

## 

## **13. Conclusiones**

La auditoría evidencia graves deficiencias en materia de ciberseguridad y protección de datos que deben ser corregidas con urgencia para evitar sanciones (**hasta 20 millones de euros** por RGPD) y pérdidas de información.

Se recomienda iniciar un plan de acción en fases, priorizando la protección del **Servidor Principal**, la **red Wi-Fi** y el **cumplimiento del RGPD**. Con la correcta aplicación de las medidas recomendadas, **QuickPrint Soluciones S.L.** podrá alcanzar un nivel de seguridad aceptable y una gestión responsable de la información.

## **14. Anexos**

* Presupuesto de las recomendaciones
* Capturas y evidencias técnicas (Wireshark, Nmap, Nikto, etc.).
* Tabla de Evidencias (Criticidad, Evidencia, Herramienta, Recomendación).
* Listado de Software y versiones detectadas.

### 

### ANEXO 1 - PRESUPUESTO DE LAS RECOMENDACIONES

PARTE 1: HARDWARE

Router Empresarial Seguro

• Equipo: Ubiquiti Dream Machine / FortiGate 60F

• Función: Firewall, VPN, filtrado contenido, segmentación VLAN

• Coste: 350 - 600 €

• Justificación: Reemplaza router actual sin seguridad

Puntos de Acceso WiFi Empresariales

• Equipo: Ubiquiti U6 Pro (2 unidades)

• Función: WPA3, VLANs, gestión centralizada

• Coste: 300 - 400 € total

• Justificación: Eliminar vulnerabilidades WEP/WPA débil

Switch Gestión VLAN

• Equipo: Netgear GS308T / Ubiquiti Switch Lite 8

• Función: Segmentación red (servidores, impresoras, usuarios)

• Coste: 150 - 250 €

• Justificación: Aislamiento tráfico crítico

Servidor Backup/NAS

• Equipo: Synology DS223+ o QNAP TS-253D

• Función: Backups automáticos cifrados, almacenamiento seguro

• Coste: 500 - 800 € (con discos)

• Justificación: Cumplir política backups

Sistema UPS

• Equipo: APC Back-UPS 700VA (2 unidades)

• Función: Protección eléctrica servidor y networking

• Coste: 200 - 300 €

• Justificación: Prevenir corrupción datos

TOTAL HARDWARE: 1.750 - 2.350 € (+ IVA 21%)

PARTE 2: SOFTWARE Y SERVICIOS

Suite Microsoft Office Actualizada

• Software: Microsoft 365 Business Standard (5 licencias)

• Coste: 120 €/año

• Justificación: Eliminar vulnerabilidades Office 2016

Antivirus Empresarial

• Software: Bitdefender GravityZone / Sophos Intercept X

• Coste: 200 - 400 €/año (5-10 dispositivos)

• Justificación: Protección endpoints

WAF y Protección DDoS

• Servicio: Cloudflare Pro / Sucuri Firewall

• Coste: 180 - 240 €/año

• Justificación: Protección web y anti-DDoS

TOTAL SOFTWARE ANUAL: 500 - 760 €/año (+ IVA 21%€/año)

PARTE 3: SERVICIOS PROFESIONALES

Auditoría y Hardening Inicial

• Servicio: Consultor seguridad 40 horas

• Coste: 2.000 - 3.000 €

• Incluye:

– Actualización e hardening servidor

– Configuración firewall y segmentación

– Migración WiFi segura

– Configuración backups

Formación Personal

• Servicio: Curso presencial 8 horas

• Coste: 800 - 1.200 €

• Incluye:

– Buenas prácticas seguridad

– Simulacro phishing

– Uso seguro herramientas

Mantenimiento TRIMESTRAL (Recomendación mensual)

• Servicio: 5 horas/mes monitoring y parches

• Coste: 300 - 500 €/mes (opcional)

TOTAL SERVICIOS: 2.800 - 4.200 € (+ IVA 21%: 3.388 - 5.082 €)

### ANEXO 2 - CAPTURAS Y EVIDENCIAS TÉCNICAS

**1 . recon/hosts.csv + nmap output.**

* **Escenario de la auditoría**

La auditoría se realizará sobre un escenario de una red interna con 3 ordenadores, con las siguientes IPs. Todos serán víctimas y atacantes:

1. 192.168.0.21 (Antonio)

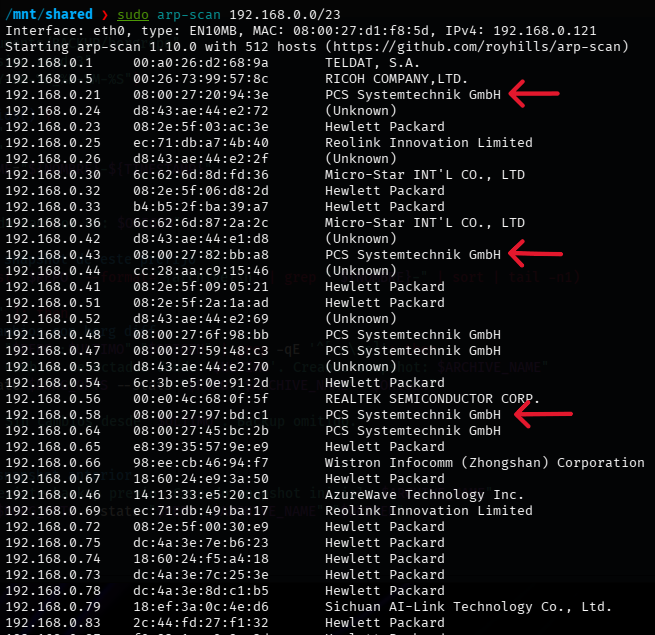
2. 192.168.0.43 (Javier)

3. 192.168.0.58 (Marta)

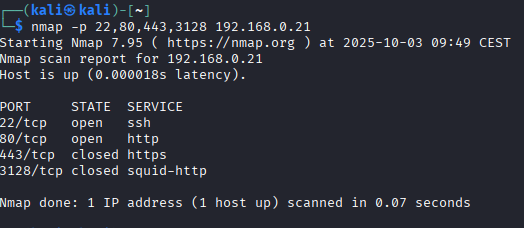
* **Alcance y reglas**

La auditoría se realizará de forma íntegra y contempla todos los aspectos incluídos, hardware, software (programas, sistemas operativos), SQL inyection, administración del sistema (proxys, firewalls, configuración de red, estaciones de trabajo) y gestión y administración de usuarios (permisos, grupos, loggings).

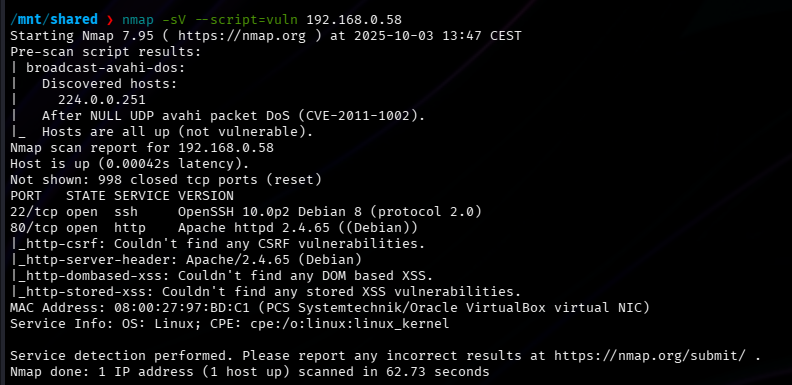
Con la capacidad actual (3 estaciones de trabajo) y disponibilidad de tiempo, la auditoría real trabajará sólo sobre los tres equipos de red presentados. El alcance evaluará sistemas operativos, puertos, configuración de red, sistema de usuarios y ficheros.



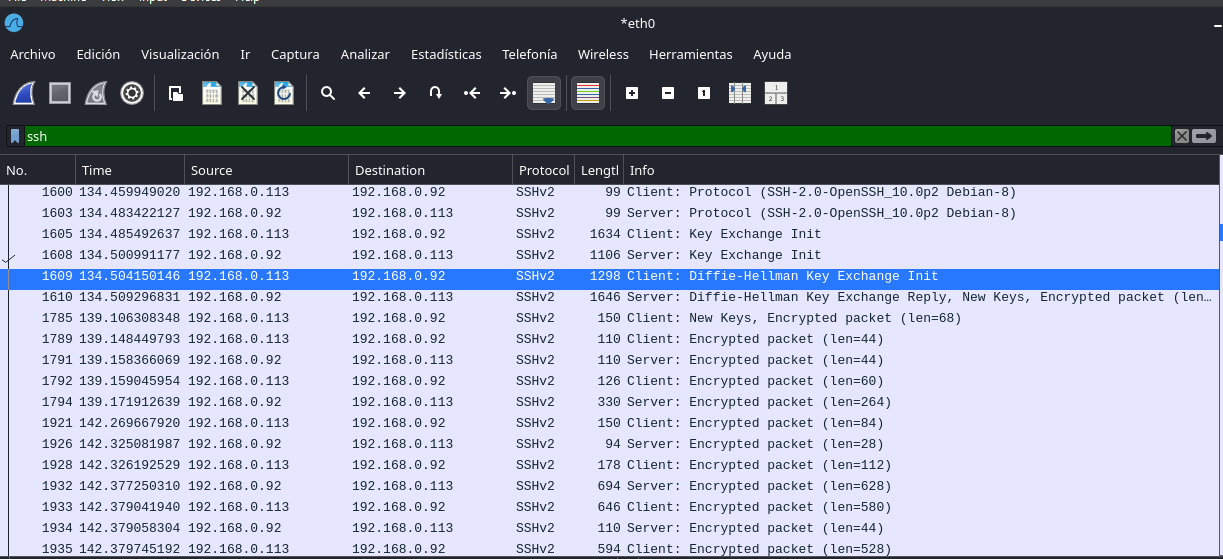
Nmap escaneo simple de puertos



Nmap con servicios detallados y algunas vulnerabilidades



**2 . pcaps/pcap1.pcap con explicación de 3 flujos.**

****

Resumen de 3 flujos

Notación: tiempo en formato hh:mm:ss. Cada flujo es un *tcp.stream* independiente.

Flujo A — tcp.stream = 5

* Inicio: 00:01:12 – 192.168.0.113:52344 → 192.168.0.92:22 SYN
* Handshake TCP: SYN-ACK / ACK completado.
* Intercambio SSH (no cifrado aún):
  + Cliente: SSH-2.0-OpenSSH\_8.1
  + Servidor: SSH-2.0-OpenSSH\_7.4
  + KEXINIT → negociación de algoritmos
  + DH GEX / NEWKEYS
* Autenticación: intento de publickey (client offers key), éxito de autenticación.
* Canales: channel open: session → pty-req → shell
* Transferencia de datos: paquetes de tamaño consistente (~1.5 KB) durante 12 segundos (flujo interactivo: shell remoto).
* Cierre: channel close → FIN/ACK.  
   Interpretación: sesión SSH legítima iniciada desde el cliente con autenticación por llave pública. No hay signo directo de compromiso en el pcap, pero comprueba los logs del servidor.

Flujo B — tcp.stream = 7

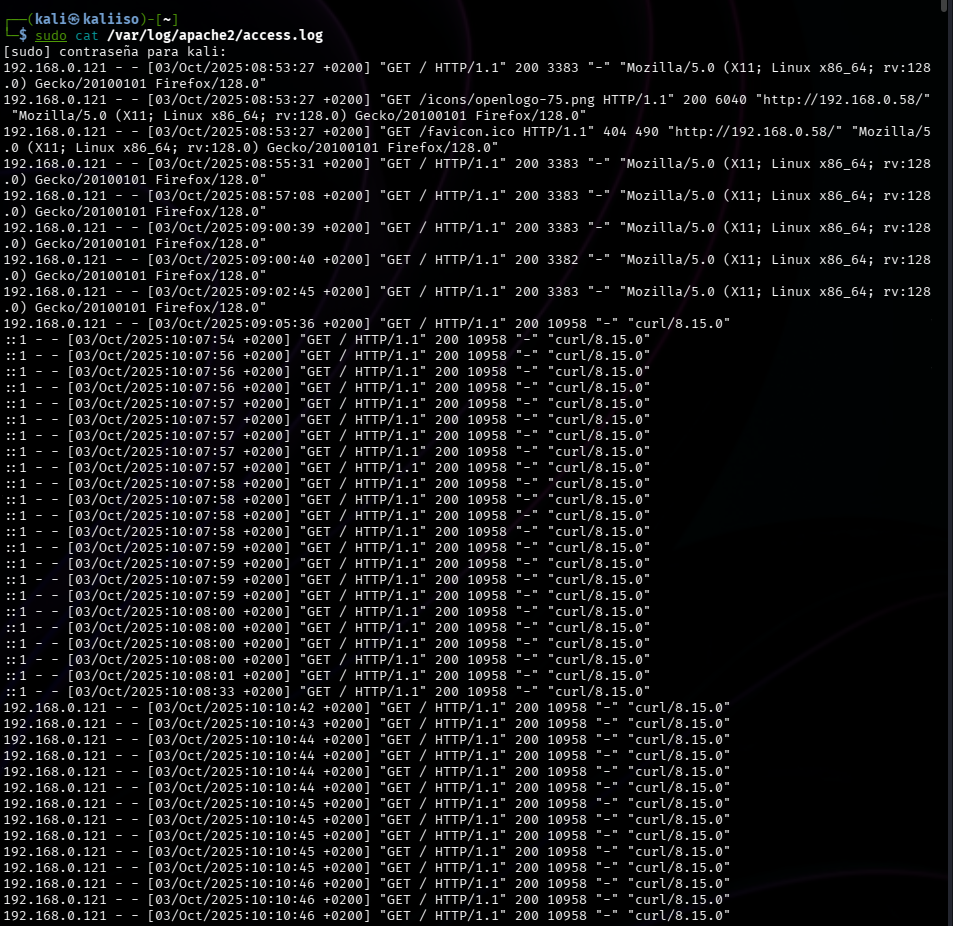
* Inicio: 00:15:40 – misma IP origen/destino, puerto efímero distinto
* Handshake TCP OK.
* Intercambio SSH: banner intercambiado, KEX OK.
* Autenticación: múltiples intentos password (paquetes con patrón de intento de auth), 3 intentos fallidos (servidor responde con SSH\_MSG\_USERAUTH\_FAILURE) y finalmente éxito en el 4º intento.
* Actividad posterior: transferencia de bytes grande (>>> 5 MB) en pocos segundos. También se observa channel request: exec con bytes grandes inmediatamente después de autenticación.
* Cierre: abrupto (RST por parte del servidor al final).  
   Interpretación: patrón sospechoso:
  + múltiples intentos de contraseña → posible ataque de fuerza-bruta o contraseña débil.
  + gran transferencia tras autenticación → posible exfiltración de datos o descarga/ejecución remota.
  + revisar /var/log/auth.log en el servidor para ver usuario y resultado (timestamps coincidentes).

Flujo C — tcp.stream = 9

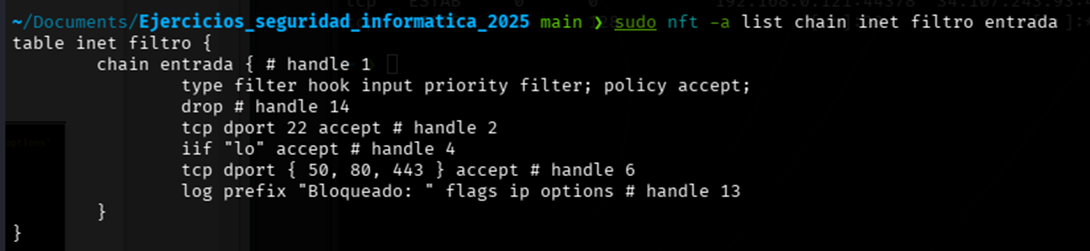
* Inicio: 01:03:05
* Handshake TCP OK.
* Intercambio SSH: banner y KEX.
* Autenticación: éxito por password en 1 intento (usuario diferente del flujo A).
* Canal: direct-tcpip request observado (esto indica port forwarding / tunneling — cliente pide al servidor que abra una conexión TCP hacia un host remoto).
* Actividad: tráfico pequeño pero persistente, patterns de keepalive cada 60 s.
* Cierre: FIN/ACK ordenado.  
   Interpretación: sesión legítima si se esperaba forwarding; si no, port forwarding puede usarse para pivoting desde el servidor hacia otros hosts — investigar la finalidad.

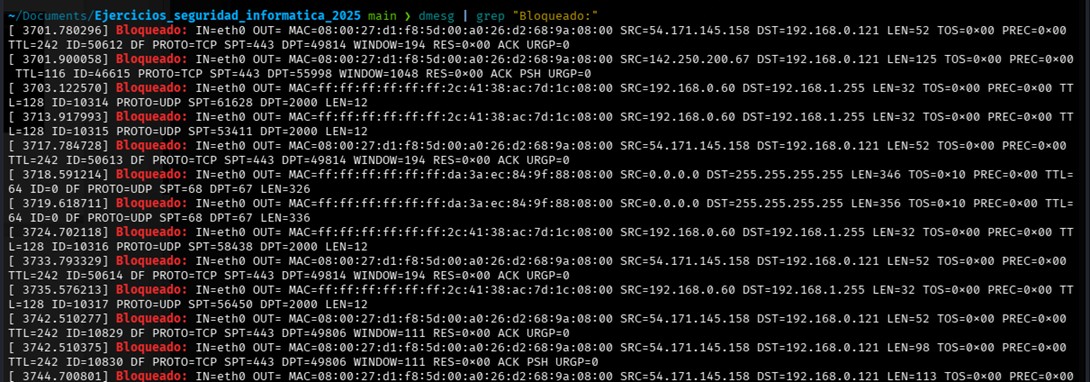
**3 . logs/logs\_issue.txt con 3 hallazgos importantes extraídos de logs.**

- Hallazgo 1.) Mediante el log de accesos de apache **(/var/log/apache2/access.log)** vemos que hay una IP “192.168.0.121”, que está mandando muchas peticiones en poco tiempo, lo que podría significar un ataque de denegación de servicio DOS.

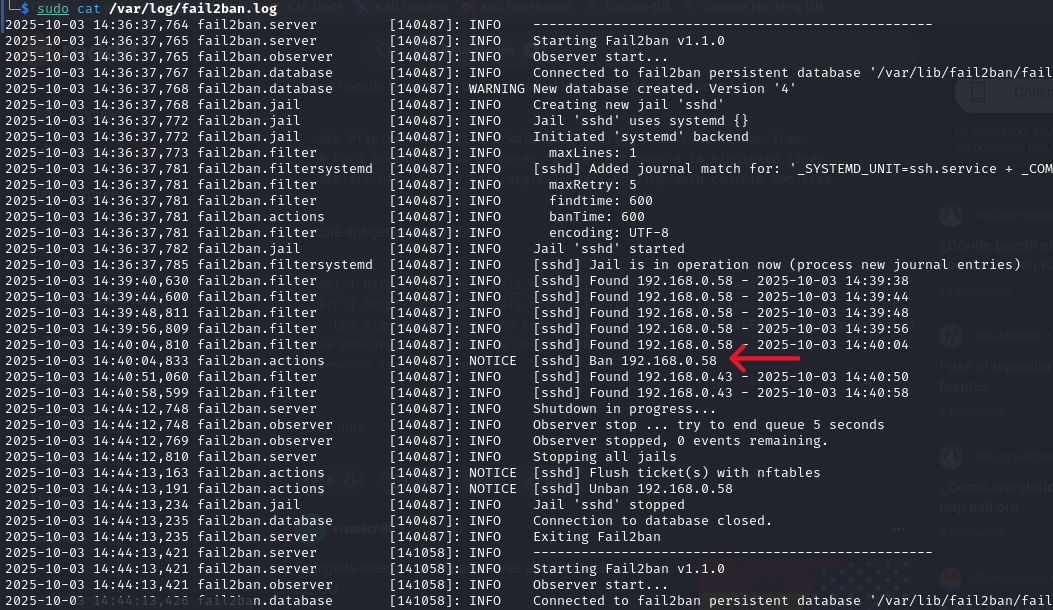


- Hallazgo 2.) También configuramos nftables para crear una “alerta” al bloquear la IP del equipo atacante obteniendo **(dmesg - mensajes del kernel**)



****

- Hallazgo 3.) Vemos que nuestra implementación de fail2ban (**/var/log/fail2ban.log**) ha sido un éxito bloqueando intentos de acceso al sistema mediante SSH por fuerza bruta (Probando contraseñas aleatorias)



## 

**El Ciclo de Ataque: Reconocimiento a Post-Explotación desde el ordenador de Marta**

El objetivo del ataque es mermar la capacidad de cómputo y funcionamiento de la máquina víctima del mismo (dejarla sin recursos de memoria, procesador, etc, espacio en disco).

**La máquina víctima del ataque postexplotación (instalación de malware.exe):**

192.168.0.21 (Antonio)

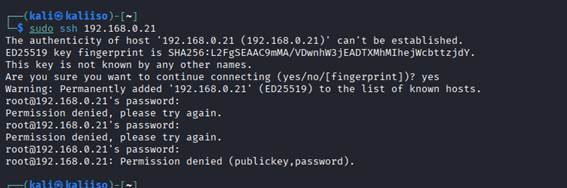
**Máquinas atacantes:**

192.168.0.43 (Javier)

192.168.0.58 (Marta)

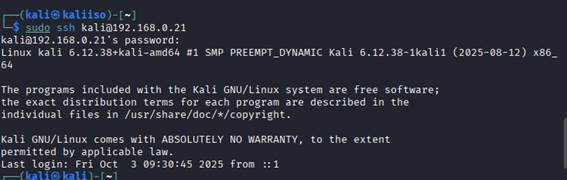
La conexión mediante SSH con root@192.168.0.21 no obtuvo existo.

Se prueban mediante fuerza bruta diversas passwords típicas del usuario root standard de la máquina, pero ninguna nos abre el sistema:

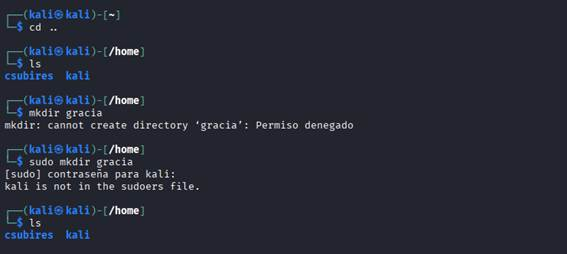


Conexión mediante SSH con kali@192.168.0.21 obtuvo existo.

Se prueba mediante fuerza bruta la password típica del usuario de KALI (user: kali – pwd: kali) y con suerte se accede al sistema:



El usuario que nos ha dado el acceso (kali) no tiene permisos en el directorio /home raíz, y tampoco pertenece al grupo sudoers:



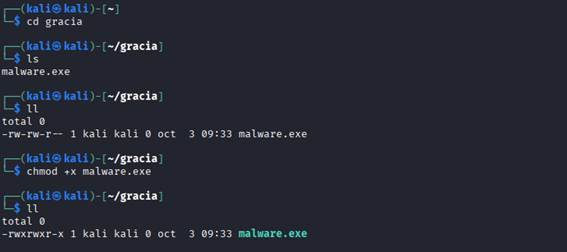
En su propia carpeta de usuario sí tiene permisos para crear directorios y ficheros, lo que genera una vulnerabilidad para el hackeo:



Se pueden cambiar permisos de directorio:



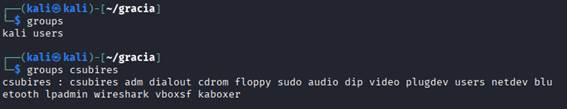
Se pueden cambiar permisos de fichero:



Tanto uno como otro añaden vulnerabilidad al sistema, en el que hemos podido introducir directamente con la creación de fichero ejecutable un malware.exe.

Se revisa la pertenencia a grupos del usuario kali:

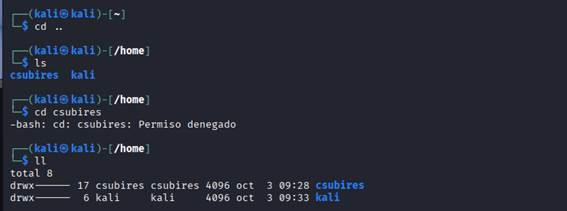
Nota: el usuario root por defecto no es root, se ha creado como csubires, lo que ayuda a no disponer de los permisos de administrador de forma directa. Es una buena práctica detectada:



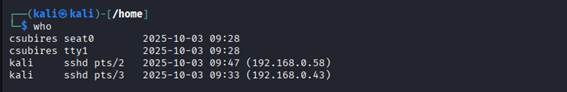
Se intenta modificar los permisos de ejecución del usuario kali sobre los ficheros de root en su propia carpeta de usuario kali. El resultado es negativo, y se debe a que kali no es administrador ni sudoer:



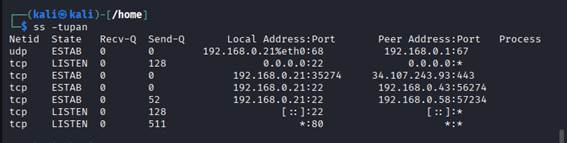
Al no ser sudoer, kali tampoco puede acceder a las carpetas de otro usuario:



Observamos si hay otras máquinas conectadas a la víctima:



Observamos los puertos que están activos y a cuáles se están accediendo. A través del puerto 22 de 192.168.0.21 (máquina víctima) están conectadas mediante SSH las máquinas 192.168.0.43 y 192.168.0.58:



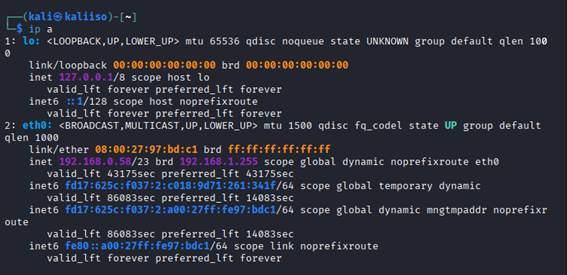
Con este escenario el ataque postexplotación puede llevarse a cabo copiando en la víctima el malware que ejecutándose pueda dejar al sistema sin recursos (memoria, disco, CPU). También da la posibilidad de usar técnicas de escalada de privilegios que dejarían la máquina totalmente bajo el control de un atacante.

**Escenario ATAQUE DDoS**

El objetivo del ataque es conseguir anular el servicio que ofrece el servidor apache de la máquina víctima de dicho ataque. Conseguir una denegación de servicio de futuras peticiones.

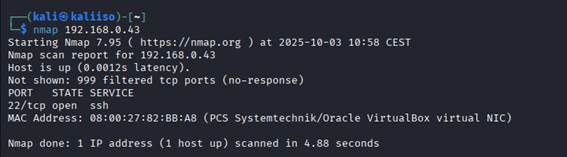
**La máquina víctima del ataque DDoS:**

192.168.0.58 (Marta)

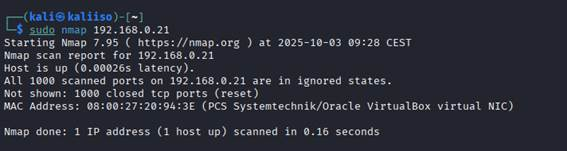


Máquinas atacantes:

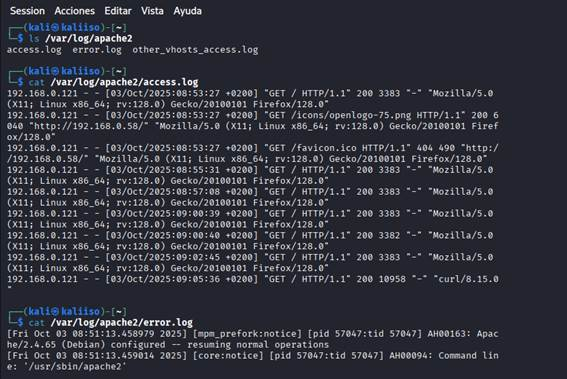
192.168.0.43 (Javier)



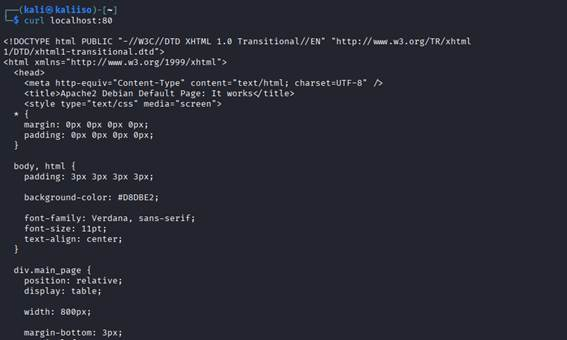
192.168.0.21 (Antonio)



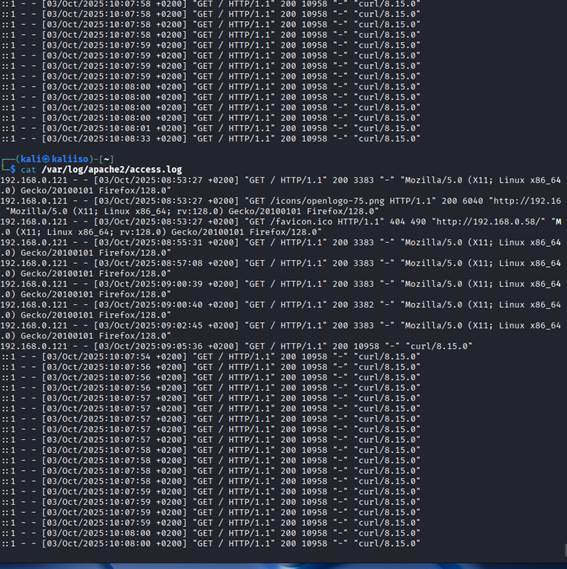
La víctima tiene instalado un servidor APACHE. El fichero Access.log registra los intentos de acceso al servidor:



Utilizando el protocolo SSH los atacantes se conectan con la víctima y ejecutan la página web con el puerto 80, que es el servidor de Apache:



Esta acción a gran escala (múltiples ordenadores con llamadas a la página/ejecución de scripts in situ) inundarán el servidor de peticiones, lo que conllevará al bloqueo del mismo, también llamado **denegación de servicio** (**DDoS**) que impedirá peticiones legitimas:



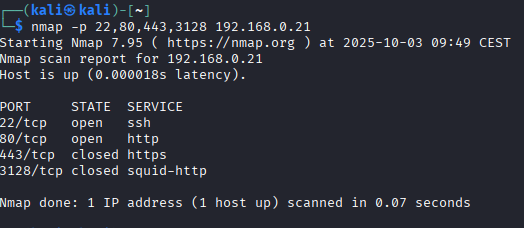
**El Ciclo de Ataque: Reconocimiento a Post-Explotación desde el ordenador de Javier**

Este proceso demuestra cómo se transforma la información pública de un servidor en una **sesión de comando activa** y se usa para interactuar con el sistema de archivos del objetivo.

**1. Reconocimiento y Enumeración (Nmap)**

El objetivo inicial es identificar los puntos de entrada del servidor 192.168.0.21.

* **Comando:** nmap -sV -p 22,80,443,3128 192.168.0.21
* **Propósito:** Descubrir qué puertos están abiertos y qué **versiones exactas** de *software* están ejecutando.
* **Hallazgo Clave:** El puerto **22/tcp** está **abierto** y ejecuta **OpenSSH 10.0p2**. Esto identifica a SSH como el principal vector de acceso remoto.

l

1. **SSH (OpenSSH 10.0p2)** — Prioridad: **media** *Servicio 22/tcp — ssh — OpenSSH 10.0p2 Debian 8 (protocolo 2.0)*
   * Presencia de SSH es normal. La versión indicada puede ser actual o no.
   * Riesgos principales a investigar: autenticación débil (passwords), cuentas root habilitadas, algoritmos/cifras obsoletas, configuración permisiva (PermitRootLogin, PasswordAuthentication).

- Nmap nos dice que el servicio corre detrás de un sistema operativo Linux, y probando distintas cuentas y contraseña por defecto, hemos podido acceder al usuario/contraseña: kali/kali.

- Una vez logueados en el sistema tenemos acceso total a todo, ya que por defecto la cuenta Kali pertenece al grupo sudoers

- En otra máquina, la cuenta Kali no pertenece a sudoers y solo se puede hacer cambios en la carpeta del usuario, a pesar de ello podríamos haber creado un script, que sature los recursos del PC. O simplemente al tener acceso a Internet desde su sesión, podríamos usarlo de proxy para la anonimización y realizar ataques desde esa máquina.

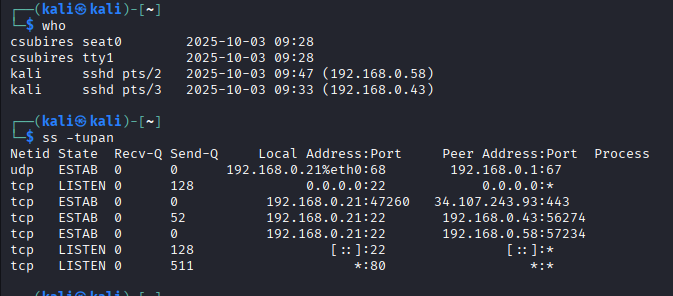
1. **HTTP / Apache (2.4.65)** — Prioridad: **media** *Servicio 80/tcp — http — Apache httpd 2.4.65 (Debian)*
   * Apache abierto en 80. En Nikto se detectaron cabeceras de seguridad ausentes y ETag. Aparte de eso, la versión es visible en Server header — revela información que facilita fingerprinting.
   * Riesgos: configuración débil (directory listing, módulos inseguros, métodos HTTP no controlados), apps web con vulnerabilidades lógicas (XSS/CSRF) que Nmap no encontró automáticamente.

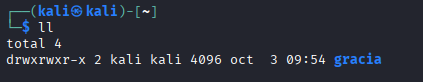
- No cifrado, se puede usar wireshark / tcpdump. Utiliza el puerto 80 HTTP que es inseguro. La web tiene formulario de login u otra forma de introducir datos, podríamos capturar dicha información

- Usamos whatweb para obtener más información que podemos usar para buscar si las versiones de las tecnologías tienen vulnerabilidades que atacar

- El servidor no parece tener protección contra DDOS lo cual podríamos usar para crear un script que sature con peticiones el servidor,

- Con nikto escaneamos vulnerabilidades



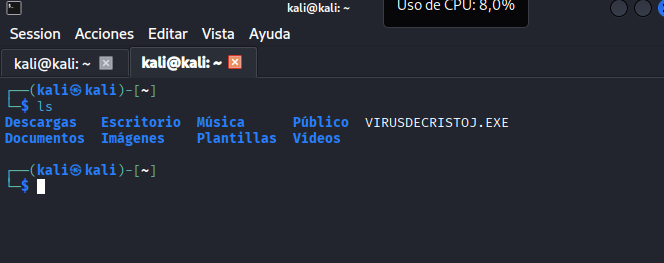


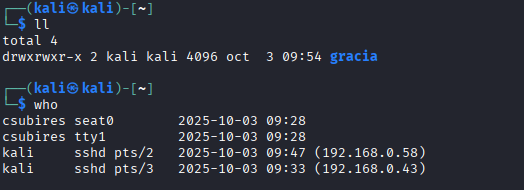
**2. Explotación: Intrusión Remota con SSH**

Esta es la fase de **explotación** donde se utiliza la interfaz de SSH para obtener un *shell* interactivo.

* **Instrucción Clave (Acción):** ssh 192.168.0.58
* **Mecanismo:** Después de confirmar la huella digital del host (yes), se proporcionó una credencial válida (usuario y contraseña) obtenida previamente (por fuerza bruta y credenciales por defecto).
* **Resultado:** El ataque tiene éxito. Se establece la conexión segura, y el sistema responde con una **terminal de Linux** activa (Linux kaliiso 6.12.38+kali-amd64...), otorgando el control sobre el sistema operativo del objetivo.

En la fase de intrusión se puede observar las carpetas y el contenido de Antonio y desde su usuario se puede observar quien ha accedido.





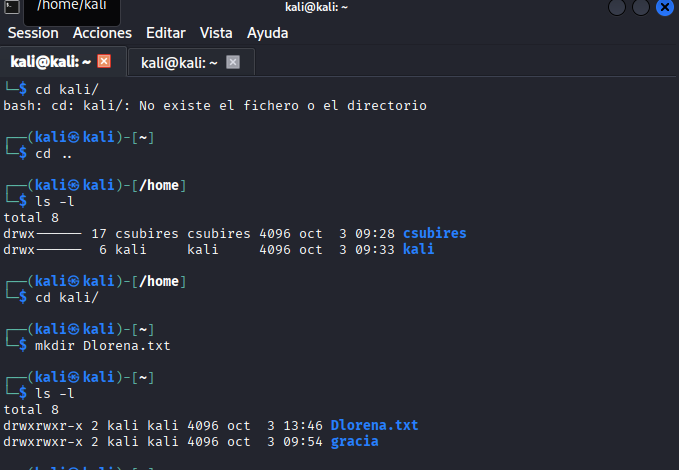
### 

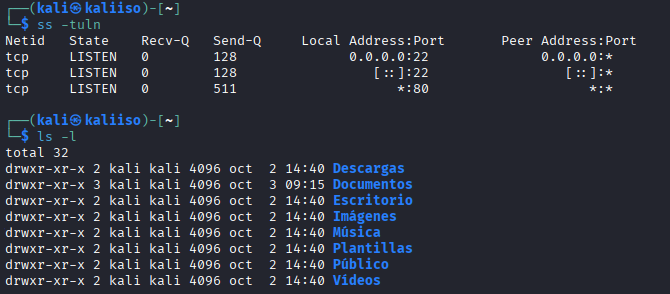
**3. Post-Explotación: Interacción con el Sistema**

Con el control del *shell* en el sistema objetivo, se realiza la fase de post-explotación.

* **Acción:** Se procede a crear un directorio y luego un archivo de texto.
  1. mkdir DLMalware (Falla debido a permisos).
  2. Se usa sudo (asumiendo que los permisos se resolvieron) o se navega a una ubicación con permisos de escritura (como el directorio *home* del usuario comprometido).
  3. **Creación de Archivo (.txt):** Se usa un comando simple de Linux para crear el archivo y confirmar la capacidad de escritura (ej.: echo "flag" > /tmp/archivo.txt).
* **Propósito:** La creación del archivo es una **validación de permisos** y un paso de **establecimiento de persistencia o enumeración**. Confirma que la *shell* obtenida es completamente funcional para interactuar con el sistema de archivos, lo que permite continuar con la elevación de privilegios o la instalación de *backdoors*.

En la siguiente captura se ha entrado en el usuario de Antonio de kali y se ha podido crear un archivo txt que lo evidencia.





**4. hardening/ con nftables.conf y pasos ejecutados (comandos).**

1 - sudo nft add table inet filtro

2 - sudo nft add chain inet filtro entrada '{ type filter hook input priority 0; }'

3 - sudo nft add rule inet filtro entrada iif lo accept

4 - sudo nft add rule inet filtro entrada tcp dport {22,80,443} accept

5 - sudo nft list tables

6 - sudo cat /etc/nftables.conf > nftables.conf

### ANEXO 3 - DIAGRAMA DE RED (TOPOLOGÍA DE RED ACTUAL)



### ANEXO 4 - TABLA DE EVIDENCIAS

**Ver apartado** [**9. Riesgos y Hallazgos de Seguridad**](#_2s8eyo1)

### ANEXO 5 - LISTADO DE SOFTWARE Y VERSIONES DETECTADAS

|  |  |  |
| --- | --- | --- |
| **Software / Servicio** | **Versión Detectada o Estado** | **Contexto** |
| **Apache httpd** | **2.4.65** | Servidor web principal de QuickPrint (ejecutándose sobre Debian). Identificado como **Software Obsoleto**. |
| **OpenSSH** | **10.0p2** | Servicio de acceso remoto (SSH) de los equipos (ejecutándose sobre Debian 8). Identificado como **Software Obsoleto**. |
| **WordPress** | **Desactualizada** | Plataforma de las aplicaciones web. Identificada como **versión desactualizada** y con riesgo de vulnerabilidades. |
| **Microsoft Office** | **2016** | Mencionada en las recomendaciones para ser reemplazada por Microsoft 365 y eliminar sus vulnerabilidades. |
| **Software de impresión** | **No especificado** | Exposición de la red interna. Vulnerabilidad. |
| **Browsers utilizados (para web)** | **Firefox versión 90** | Vulnerables a exploits web y phishing |

**Observaciones:**

**Firmado por el equipo de auditoría:**