

# Informe

# Auditoria de Red

1. Resumen ejecutivo	4
2. Alcance y limitaciones	4
2.1 Alcance	4
2.2 Limitaciones	4
3. Autorización y consideraciones éticas	4
4. Metodología y herramientas	5
4.1 Metodología	5
4.2 Herramientas	5
5. Inventario de activos	5
6. Hallazgos	5
6.1 Vulnerabilidad crítica – Detalle	6
7. Pruebas MitM y Análisis de tráfico capturado	6
8. Evaluación de riesgo y triaje	7
9. Recomendaciones	7
10. Plan de remediación sugerido	7
11. Conclusiones	8
12. Anexos	8

## Informe Auditoria de Red

---

Versión	Fecha	Auditor	Cambios
1.0	13.10.2025	Ignacio Elízaga	XXXXXXX

## 1. Resumen ejecutivo

Este informe presenta los resultados de la auditoría interna realizada sobre mi red local. El objetivo fue evaluar la postura de seguridad de la infraestructura, identificar activos y servicios expuestos, identificar vulnerabilidades remarcables y comprobar la posibilidad de interceptación de tráfico mediante técnicas Man-in-the-Middle (MitM).

En síntesis:

- Alcance: Red LAN doméstica.
- Objetivo principal: enumeración de activos, análisis de vulnerabilidades y pruebas MitM controladas.
- Resultado: Se identificaron servicios expuestos y al menos una vulnerabilidad de criticidad alta (detalles en sección 8). Se demostró la viabilidad técnica de un ataque MitM en el entorno de pruebas; se capturaron paquetes que contienen tráfico no cifrado (o cifrado) en protocolos inseguros.

## 2. Alcance y limitaciones

### 2.1 Alcance

La auditoría incluyó: reconocimiento de la red (descubrimiento de hosts, identificación por MAC/OUI, fingerprinting de SO), escaneos de puertos y servicios, análisis automatizado de vulnerabilidades y una prueba MitM controlada entre equipo X y equipo Y. No se realizaron pruebas destructivas ni explotación activa que pudieran causar indisponibilidad.

### 2.2 Limitaciones

- Pruebas realizadas únicamente en la red proporcionada por el cliente.
- Actividades se limitaron a técnicas no disruptivas salvo MitM con consentimiento.
- Ciertas pruebas pueden estar sujetas a false positives/negatives de las herramientas automáticas.

## 3. Autorización y consideraciones éticas

Se dispone de autorización expresa para realizar las pruebas en la red. El equipo auditor ha seguido prácticas éticas: comunicación previa, ventana de pruebas acordada, y medidas para minimizar impacto. Cualquier dato sensible capturado se ha tratado confidencialmente.

Se adjunta autorización (firma/email): Ignacio Elízaga Vernis

## 4. Metodología y herramientas

### 4.1 Metodología

La prueba siguió las fases siguientes: planificación y autorización, reconocimiento pasivo/activo, enumeración y fingerprinting, análisis de vulnerabilidades automatizado, triaje y priorización de riesgos, prueba MitM controlada y recolección de evidencias. Se documentó cada paso mediante capturas para evidencia.

### 4.2 Herramientas

- arp-scan (para los hosts)
- Ifconfig /ip route / ipconfig (Comprobaciones IP)
- nmap (-sV, -O etc..)
- OpenVAS para sacar el análisis de vulnerabilidades
- arpspoof / ettercap (ARP poisoning)
- Wireshark (captura y análisis de tráfico)

## 5. Inventario de activos

Se adjunta en apéndice el inventario completo extraído. A continuación se muestra un resumen de los activos críticos detectados:

IP	MAC	Fabricante (OUI)	Hostname	SO estimado	Rol/Comentario
<b>192.168.1.1</b>	60:8d:26:ef:d3:09	Arcadyan Corporation	router.local	Firmware (Embedded Linux)	Router – Gateway objetivo
<b>192.168.1.22</b>		Dell	host-alumno (Kali)	Windows 10 (estimado)	Kali
<b>192.168.1.17</b>	bc:f4:d4:0d:ab:3f	MSI	Host-alumno(or denador)	Windows 10 (estimado)	Ordenador
<b>192.168.1.28</b>	aa:47:1e:20:3d:c4	IOS 15	Host-alumno (movil)	IOS 15	Movil atacante

## 6. Hallazgos

Resumen ejecutivo de hallazgos críticos y altos. Se listan a continuación las vulnerabilidades priorizadas por criticidad y su impacto potencial:

ID	Vulnerabilidad	CVE	CVSS	Servicio/Host	Prioridad / Recomendación rápida
F-01	Samba - Remote Code Execution	CVE-2017-7494	10.0 (CRÍTICA)	192.168.1.10:445	Actualizar Samba a versión parcheada; restringir acceso SMB a VLAN interna.
F-02	HTTP sin TLS - credenciales en texto plano	N/A	7.1 (ALTA)	192.168.1.10:80	Migrar a HTTPS, usar HSTS y configurar certificados válidos.
F-03	Panel de administración con credenciales por defecto o débiles	N/a	7.5(ALTA)	192.168.1.1:80	Cambiar inmediatamente las credenciales por defecto del router (por ejemplo, <i>admin/admin</i> o <i>1234</i> ), aplicar contraseñas robustas y únicas.
F-04	UPnP y servicios de gestión remota expuestos	N/A	5.3(MEDIA)	192.168.1.1	Revisar las configuraciones del router y aplicar reglas de firewall internas para impedir el acceso externo a servicios de gestión. Comprobar logs del router tras aplicar los cambios para confirmar que no hay intentos de conexión.
F-05	ICMP y TCP Timestamps habilitados(info rmación del sistema expuesta)	N/A	3.7 (BAJA)	192.168.1.1 (ICMP / TCP)	Deshabilitar los <b>timestamps</b> TCP si es posible desde la configuración

## Informe Auditoria de Red

---

					avanzada del router.
<b>F-06</b>	SSL/TLS — Weak cipher suites / suites débiles	CVE-2013-2566, CVE-2015-2808, CVE-2015-4000 (ref.)	5.9 (Medium)	192.168.1.1:8443	Eliminar suites débiles; configurar solo suites recomendadas.

### 6.1 Vulnerabilidad crítica – Detalle

ID: F-01

Nombre y CVE: Samba - Remote Code Execution (CVE-2017-7494)

Descripción: Vulnerabilidad que permite la ejecución remota de código explotando una carga de modulos no segura en versiones afectadas de Samba. Impacto: ejecución remota, pérdida de confidencialidad e integridad, posible pivot hacia otros dispositivos en la red.

Evidencia: salida del escáner OpenVAS / Nessus y resultados Nmap adjuntos. Referencias: NVD, advisory vendor.

Recomendación técnica: aplicar parche oficial, restringir acceso al puerto 445 mediante ACLs, y monitorizar conexiones SMB inusuales.

ID: F-02

Nombre y CVE: HTTP sin TLS — credenciales en texto plano (N/A)

Descripción: La página de administración usa HTTP y envía usuarios/contraseñas sin cifrar. Cualquiera en la red puede ver esos datos si intercepta el tráfico.

Evidencia: Capturas de Wireshark muestran peticiones a /login.htm con el campo de contraseña en claro; aparece en el informe de escaneo.

Recomendación técnica: Activar HTTPS en el router, forzar redirección de HTTP a HTTPS y usar un certificado válido. Evitar formularios de login en HTTP.

ID: F-03

Nombre y CVE: Credenciales por defecto o débiles en el router (N/A)

## Informe Auditoria de Red

---

**Descripción:** El router tiene usuario/contraseña por defecto o contraseñas fáciles. Eso facilita el acceso no autorizado.

**Evidencia:** Entrada del escáner que indica configuración por defecto / credenciales débiles en la interfaz de administración.

**Recomendación técnica:** Cambiar las credenciales por otras seguras (contraseña larga y única), desactivar cuentas innecesarias y comprobar que el acceso remoto esté deshabilitado.

ID: F-04

Nombre y CVE: UPnP y administración remota expuestos (N/A)

**Descripción:** Servicios como UPnP o la gestión remota están activos y pueden abrir puertos o permitir cambios desde la red/Internet.

**Evidencia:** Detección de servicios UPnP/TR-064 y puertos de gestión abiertos en el escaneo.

**Recomendación técnica:** Desactivar UPnP si no se usa, bloquear la administración desde WAN y limitar acceso a la interfaz solo a la LAN o a IPs confiables.

ID: F-05

Nombre y CVE: ICMP/TCP timestamps habilitados (N/A)

**Descripción:** El router responde con timestamps y da información de uptime que ayuda a perfilar el dispositivo.

**Evidencia:** Resultado del escáner que muestra timestamps activos en ICMP/TCP.

**Recomendación técnica:** Desactivar timestamps si es posible y filtrar respuestas ICMP no necesarias para reducir la información expuesta.

ID: F-06

Nombre y CVE: Transmisión de credenciales por HTTP (N/A)

**Descripción:** La página de administración del router envía usuario y contraseña por HTTP, sin cifrar. Cualquiera en la red podría captarlo si hace sniffing.

**Evidencia:** Captura de Wireshark mostrando peticiones a /login.htm con la contraseña en claro; OpenVAS detectó transmisión en texto claro en el puerto 80 de 192.168.1.1.

Recomendación técnica: Activar HTTPS y forzar redirección HTTP → HTTPS. Si no se puede, restringir el acceso al panel a IPs de administración y desactivar el acceso remoto (WAN).

## 7. Pruebas MitM y Análisis de tráfico capturado

Se realizó una prueba de ARP spoofing con consentimiento entre el host objetivo y el router para evaluar la posibilidad de interceptación de tráfico. Se documentaron las acciones y se conservaron los .pcap como evidencia.

Resumen: se capturó tráfico HTTP que contenía formularios y headers sin cifrar. No se realizó explotación adicional; las credenciales capturadas se trataron como PoC y no se difundieron.

Comandos utilizados (resumen):

Ettercap -g abre el entorno grafico haces el scaneo

Se utiliza wireshark

## 8. Evaluación de riesgo y triaje

Durante el análisis se identificaron dos vulnerabilidades críticas (Samba RCE y HTTP sin cifrado), una vulnerabilidad alta (credenciales por defecto), una media (UPnP activo) y una baja (timestamps habilitados).

Las vulnerabilidades críticas requieren atención inmediata, ya que permiten ejecución remota de código o exposición de credenciales. Las de prioridad media y baja pueden abordarse posteriormente mediante ajustes de configuración y buenas prácticas de mantenimiento.

## 9. Recomendaciones

- Aplicar parches de seguridad y actualizar software a versiones soportadas.
- Forzar el uso de TLS/HTTPS para todos los servicios web; deshabilitar HTTP cuando sea posible.
- Deshabilitar servicios innecesarios y aplicar principio de mínimo privilegio.
- Segmentar la red: red de invitados y VLANs para IoT separados del segmento corporativo/host.
- Configurar firewall/ACLs para limitar accesos a servicios internos (ej. SMB, RDP).

- Habilitar autenticación multifactor donde sea posible.
- Implementar monitorización (IDS/IPS), y revisar logs de forma periódica.

## 10. Plan de remediación sugerido

Se sugiere el siguiente calendario de acciones:

Acción	Prioridad	Plazo sugerido
<b>Aplicar parches críticos (p. ej., Samba)</b>	Alta	0-7 días
<b>Migrar servicios HTTP a HTTPS</b>	Alta	7-30 días
<b>Segmentación de red (VLANs)</b>	Media	30-90 días
<b>Cambiar credenciales por defecto y establecer contraseñas seguras</b>	Alta	0-7 días
<b>Deshabilitar servicios innecesarios (UPnP, gestión remota)</b>	Media	7-30 días
<b>Desactivar timestamps y filtrar ICMP innecesario</b>	Baja	30-90 días

## 11. Conclusiones

La auditoría ha identificado áreas críticas que requieren atención inmediata, así como mejoras de configuración y de proceso para reducir la superficie de ataque. El riesgo principal se deriva de servicios expuestos y tráfico no cifrado.

## 12. Anexos

- A. Comandos completos y salidas (anexar archivos):
- B. Se adjunta junto a la entrega un Word con la mayoría de los comandos utilizados para llevar a cabo la práctica y un PDF de OpenV con las vulnerabilidades del router de mi casa.
- C. Evidencias: mitm\_capture.pcap, capturas de Wireshark, capturas de Nmap