UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE INGENIERIA INDUSTRIAL
CARRERA DE INGENIERÍA EN TELEINFORMÁTICA

TRABAJO DE TITULACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN TELEINFORMATICA

ÁREA
REDES INTELIGENTES

TEMA
“ANÁLISIS DE LAS MALAS PRÁCTICAS EN ACTIVE DIRECTORY MEDIANTE HERRAMIENTAS DE PENTESTING Y MITIGACIÓN DE VULNERABILIDADES A TRAVÉS DE UN MARCO METODOLÓGICO DE SEGURIDAD.”

AUTOR
AYOVI GRUEZO JERSON PAUL

DIRECTORA DEL TRABAJO
ING. CASTILLO LEÓN ROSA ELIZABETH, MG.

GUAYAQUIL, ABRIL 2021

ANEXO XI.- FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:			
"ANÁLISIS DE LAS MALAS PRÁCTICAS EN ACTIVE DIRECTORY MEDIANTE HERRAMIENTAS DE PENTESTING Y MITIGACIÓN DE VULNERABILIDADES A TRAVÉS DE UN MARCO METODOLÓGICO DE SEGURIDAD."			
AUTOR(ES) (apellidos/nombres):	AYOVI GRUEZO JERSON PAUL		
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):	ING. PLAZA VARGAS ANGEL MARCEL, MSC / ING. CASTILLO LEÓN ROSA ELIZABETH, MG		
INSTITUCIÓN:	UNIVERSIDAD DE GUAYAQUIL		
UNIDAD/FACULTAD:	FACULTAD DE INGENIERÍA INDUSTRIAL		
MAESTRÍA/ESPECIALIDAD:			
GRADO OBTENIDO:	INGENIERO EN TELEINFORMÁTICA		
FECHA DE PUBLICACIÓN:	27 de septiembre del 2021	No. DE PÁGINAS:	133
ÁREAS TEMÁTICAS:	REDES INTELIGENTES		
PALABRAS CLAVES/ KEYWORDS:	Seguridad, Malas prácticas, virtualización, políticas, pentesting / Security, Bad practices, virtualization, policies, pentesting.		

RESUMEN. - Actualmente las empresas han puesto en práctica el uso de los directorios activos como Active Directory para la centralización de la información con el fin de mantener un mayor control de la información. Sin embargo, existe una cantidad considerable de antecedentes que reflejan incidentes de seguridad en los servicios de Active Directory. Calificado como activo crítico de la organización debido a que durante la fase de implementación y configuración se desarrolla con mala práctica, lo que genera una serie de vulnerabilidades que son explotadas por agentes externos. Frente a esto se sustenta el objetivo principal de este trabajo, el cual es proveer el conocimiento necesario de seguridad de la información que sirva de guía para una correcta administración de los servicios de Active Directory, en base al análisis de vulnerabilidades utilizando métodos de pentesting en un

ambiente controlado que emule escenarios más comunes de malas prácticas, así mismo definir lineamientos para el desarrollo de políticas de seguridad de la información que cumplan con los objetivos de la organización.

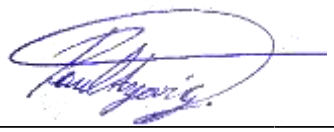
ABSTRACT. - Currently, companies have implemented the use of active directories such as Active Directory for the centralization of information in order to maintain greater control of information. However, there is a considerable amount of precedents that reflect security incidents in Active Directory services. Therefore, it is qualified as a critical asset of the organization due to the fact that during the implementation and configuration phase it is developed with bad practices, which generates a series of vulnerabilities that are exploited by external agents. The main objective of this work is to provide the necessary information security knowledge to serve as a guide for a correct management of Active Directory services, based on the analysis of vulnerabilities using pentesting methods in a controlled environment that emulates the most common scenarios of bad practices, as well as to define guidelines for the development of information security policies that meet the objectives of the organization

ADJUNTO PDF:	SI (X)	NO
CONTACTO CON AUTOR/ES:	Teléfono: 0982796377	E-mail: Jerson.ayovig@ug.edu.ec
CONTACTO CON LA INSTITUCIÓN:	Nombre: Ing. Ramón Maquiló Nicola	
	Teléfono: 593-2658128	
	E-mail: direccionTi@ug.edu.ec	

ANEXO XII.- DECLARACIÓN DE AUTORÍA Y DE AUTORIZACIÓN DE LICENCIA GRATUITA INTRANSFERIBLE Y NO EXCLUSIVA PARA EL USO NO COMERCIAL DE LA OBRA CON FINES NO ACADÉMICOS
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

LICENCIA GRATUITA INTRANSFERIBLE Y NO COMERCIAL DE LA OBRA CON FINES NO ACADÉMICOS

Yo, **AYOVI GRUEZO JERSON PAUL**, con C.C. No. **0850242868**, certifico que los contenidos desarrollados en este trabajo de titulación, cuyo título es **"ANÁLISIS DE LAS MALAS PRÁCTICAS EN ACTIVE DIRECTORY MEDIANTE HERRAMIENTAS DE PENTESTING Y MITIGACIÓN DE VULNERABILIDADES A TRAVÉS DE UN MARCO METODOLÓGICO DE SEGURIDAD"** son de mi absoluta propiedad y responsabilidad, en conformidad al Artículo 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN*, autorizo la utilización de una licencia gratuita intransferible, para el uso no comercial de la presente obra a favor de la Universidad de Guayaquil.



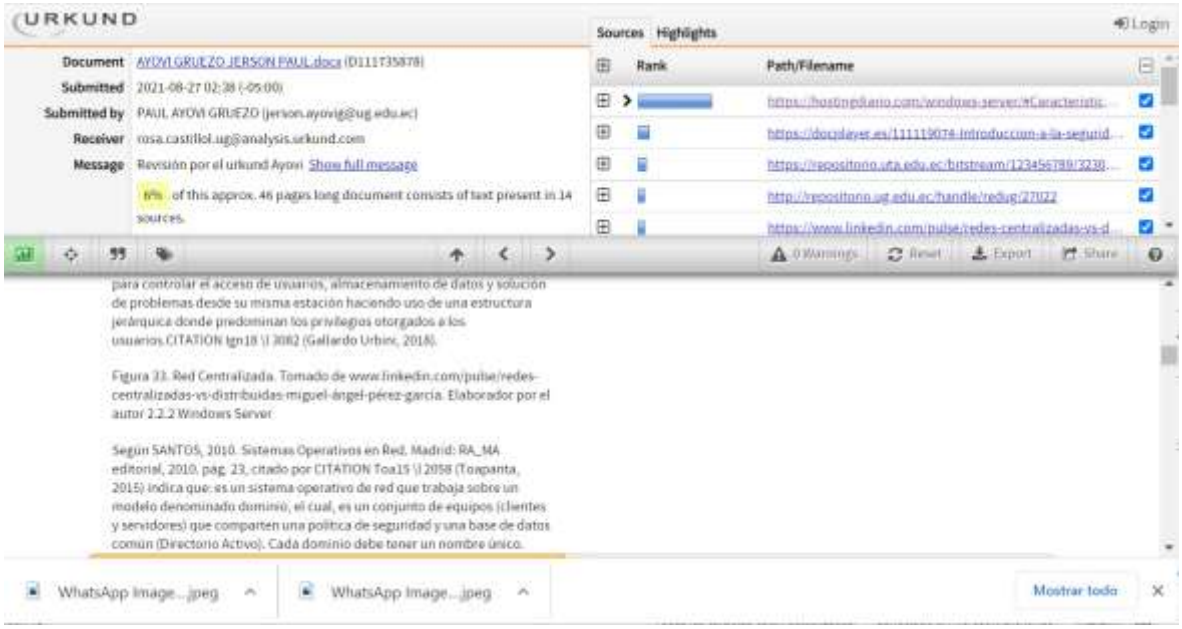
AYOVI GRUEZO JERSON PAUL
C.C. No. 0850242868

ANEXO VII.- CERTIFICADO PORCENTAJE DE SIMILITUD

FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

Habiendo sido nombrado ING. ROSA ELIZABETH CASTILLO LEÓN MG, tutor del trabajo de titulación certifico que el presente trabajo de titulación ha sido elaborado por AYOVI GRUEZO JERSON PAUL, con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERO EN TELEINFORMÁTICA. .

Se informa que el trabajo de titulación: ANÁLISIS DE LAS MALAS PRÁCTICAS EN ACTIVE DIRECTORY MEDIANTE HERRAMIENTAS DE PENTESTING Y MITIGACIÓN DE VULNERABILIDADES A TRAVÉS DE UN MARCO METODOLÓGICO DE SEGURIDAD, ha sido orientado durante todo el periodo de ejecución en el programa Antiplagio URKUND quedandoel 6% de coincidencia.



https://secure.urkund.com/view/106467316-365479-130249

Firmado electrónicamente por:
ROSA ELIZABETH CASTILLO LEON

ING. ROSA ELIZABETH CASTILLO LEÓNDOCENTE TUTOR
C.C. 0922372610
FECHA: 13 DE SEPTIEMBRE DE 2021

ANEXO VI. - CERTIFICADO DEL DOCENTE-TUTOR DEL TRABAJO DE TITULACIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

Guayaquil 13 de septiembre de 2021,

Sr (a).
Ing. Annabelle Lizarzaburu Mora, MG.
Director (a) de Carrera Ingeniería en Teleinformática / Telemática
FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL
Ciudad. –

De mis consideraciones:

Envío a Ud. el Informe correspondiente a la tutoría realizada al Trabajo de Titulación ANÁLISIS DELAS MALAS PRÁCTICAS EN ACTIVE DIRECTORY MEDIANTE HERRAMIENTAS DE PENTESTING Y MITIGACIÓN DE VULNERABILIDADES A TRAVÉS DE UN MARCO METODOLÓGICO DE SEGURIDAD del estudiante AYOVI GRUEZO JERSON PAUL, indicandoque ha cumplido con todos los parámetros establecidos en la normativa vigente:

- El trabajo es el resultado de una investigación.
- El estudiante demuestra conocimiento profesional integral.
- El trabajo presenta una propuesta en el área de conocimiento.
- El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se adjunta el certificado de porcentaje de similitud y la valoración del trabajo de titulación con la respectiva calificación.

Dando por concluida esta tutoría de trabajo de titulación, **CERTIFICO,** para los fines pertinentes,que el estudiante está apto para continuar con el proceso de revisión final.

Atentamente,

Firmado electrónicamente por:
ROSAELIZABETH CASTILLO LEON

ING. ROSA CASTILLO LEÓN
TUTOR DE TRABAJO DE TITULACIÓNC.C. 0922372619
FECHA: 13 DE SEPTIEMBRE DE 2021

ANEXO VIII.- INFORME DEL DOCENTE REVISOR
FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA

Guayaquil, 21 de septiembre de 2021.

Sr (a).
Ing. Annabelle Lizarzaburu Mora, MG.

Director (a) de Carrera Ingeniería en Teleinformática / Telemática
FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL

Ciudad. -

De mis consideraciones:

Envío a Ud. el informe correspondiente a la REVISIÓN FINAL del Trabajo de Titulación **"ANÁLISIS DE LAS MALAS PRÁCTICAS EN ACTIVE DIRECTORY MEDIANTE HERRAMIENTAS DE PENTESTING Y MITIGACIÓN DE VULNERABILIDADES A TRAVÉS DE UN MARCO METODOLÓGICO DE SEGURIDAD"** del estudiante **AYOVI GRUEZO JERSON PAUL**. Las gestiones realizadas me permiten indicar que el trabajo fue revisado considerando todos los parámetros establecidos en las normativas vigentes, en el cumplimento de los siguientes aspectos:

Cumplimiento de requisitos de forma:
El título tiene un máximo de 24 palabras.
La memoria escrita se ajusta a la estructura establecida.
El documento se ajusta a las normas de escritura científica seleccionadas por la Facultad.La investigación es pertinente con la línea y sublíneas de investigación de la carrera.
Los soportes teóricos son de máximo 5
años.La propuesta presentada es pertinente.

Cumplimiento con el Reglamento de Régimen Académico:
El trabajo es el resultado de una investigación.
El estudiante demuestra conocimiento profesional integral.
El trabajo presenta una propuesta en el área de
conocimiento.
El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se indica que fue revisado, el certificado de porcentaje de similitud, la valoración del tutor, así como de las páginas preliminares solicitadas, lo cual indica el que el trabajo de investigación cumple con los requisitos exigidos.

Una vez concluida esta revisión, considero que el estudiante está apto para continuar el proceso de titulación. Particular que comunicamos a usted para los fines pertinentes.

Atentamente,

Firmado electrónicamente por:
ANGEL MARCEL PLAZA VARGAS

ING. ANGEL MARCEL PLAZA VARGAS, MSC.
C.C:0915953665 FECHA: 21 de septiembre de 2021

Dedicatoria

Dedico el presente trabajo de investigación, a mis padres Viviana Gruezo y Ramon Ayovi, quienes confiaron de principio a fin en mis capacidades, también incluyo a mis hermanos, amigos y compañeros de universidad que supieron dármela mano cuando más lo necesité y para todos quienes han sido parte de este proceso.

Dedicado a mí y cada uno de los días en que no me rendí y supe dar lo mejor, recordando que cada noche y cada esfuerzo se ve hoy reflejado en este trabajo de investigación de fin de carrera.

Agradecimiento

En primer lugar, agradezco a Dios porque a pesar de la adversidad me dio la fuerza para mantenerme de pie durante este largo camino, seguido agradezco a mis padres y hermanos quienes me supieron dar el apoyo en todo momento de mi carrera y un agradecimiento especial a mi tía Carina Cuellar quien me supo abrir las puertas de su hogar y tratarme como uno más de sus hijos hasta el último de sus días. A uno de mis grandes amigos y colega originario de esmeraldas, ingeniero Bryan Solís Angulo que supo compartir sus conocimientos durante varios semestres de la carrera, y así mismo las personas que desde que llegue esta ciudad fueron formando parte de mi vida y dieron su aporte en pequeña y gran medida, no sin olvidar a mis compañeros y maestros de la universidad que fueron testigos más cercanos del esfuerzo durante la carrera universitaria y su apoyo académico fue fundamental, a todos ustedes gracias.

Índice General

Capitulo III

La propuesta

Índice de Tablas

Índice de Figuras

Índice de Anexos

ANEXO XIII.- RESUMEN DEL TRABAJO DE TITULACIÓN (ESPAÑOL)
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

"ANÁLISIS DE LAS MALAS PRÁCTICAS EN ACTIVE DIRECTORY MEDIANTE HERRAMIENTAS DE PENTESTING Y MITIGACIÓN DE VULNERABILIDADES A TRAVÉS DE UN MARCO METODOLÓGICO DE SEGURIDAD."

Autor: Ayovi Gruezo Jerson Paul

Tutor: Ing. Castillo León Rosa Elizabeth, MG.

Resumen

Actualmente las empresas han puesto en práctica el uso de los directorios activos como Active Directory para la centralización de la información con el fin de mantener un mayor control de la información. Sin embargo, existe una cantidad considerable de antecedentes que reflejan incidentes de seguridad en los servicios de Active Directory. Por lo que es calificado como activo crítico de la organización debido a que durante la fase de implementación y configuración se desarrolla con mala práctica, lo que genera una serie de vulnerabilidades que son explotadas por agentes externos. Frente a esto se sustenta el objetivo principal de este trabajo, el cual es proveer el conocimiento necesario de seguridad de la información que sirva de guía para una correcta administración de los servicios de Active Directory, en base al análisis de vulnerabilidades utilizando métodos de pentesting en un ambiente controlado que emule escenarios más comunes de malas prácticas, así mismo definir lineamientos para el desarrollo de políticas de seguridad de la información que cumplan con los objetivos de la organización.

Palabras Claves: Seguridad, Malas prácticas, virtualización, políticas, pentesting.

ANEXO XIV.- RESUMEN DEL TRABAJO DE TITULACIÓN (ÍNGLES)
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

"ANALYSIS OF BAD PRACTICES IN ACTIVE DIRECTORY THROUGH PENTESTING TOOLS AND VULNERABILITY MITIGATION THROUGH A SECURITY METHODOLOGICAL FRAMEWORK"

Autor: Ayovi Gruezo Jerson Paul

Tutor: SE Castillo León Rosa Elizabeth, MG.

Currently, companies have implemented the use of active directories such as Active Directory for the centralization of information in order to maintain greater control of information. However, there is a considerable amount of precedents that reflect security incidents in Active Directory services. Therefore, it is qualified as a critical asset of the organization due to the fact that during the implementation and configuration phase it is developed with bad practices, which generates a series of vulnerabilities that are exploited by external agents. The main objective of this work is to provide the necessary information security knowledge to serve as a guide for a correct management of Active Directory services, based on the analysis of vulnerabilities using pentesting methods in a controlled environment that emulates the most common scenarios of bad practices, as well as to define guidelines for the development of information security policies that meet the objectives of the organization

Keywords: Security, Bad practices, virtualization, policies, pentesting.

Introducción

En la actualidad los sistemas informáticos han experimentado grandes cambios en cuanto a nivel de infraestructura de red interna se refiere, donde las organizaciones hacen uso de este elemento para optimizar los procesos relacionados con el procesamiento y almacenamiento de información, en la búsqueda de aumentar su rendimiento en tiempos de espera entre actividades que se desarrollen a diario, mismas que se han convertido en uno de los pilares fundamentales del trabajo en equipo con la posibilidad de compartir información entre varias estaciones de trabajo.

Partiendo de la idea del compartimiento de información en las redes internas como factor de vital importancia para la optimización de procesos, se hace necesario indicar que la seguridad de este tipo de ambientes que manejan un entorno centralizado se convierte evidentemente en un objetivo deseado por ciberatacantes que buscan el robo de información o tener un acceso ilegal a los recursos de la red. Por consiguiente, si una organización parte de un crecimiento y mejora de su infraestructura de red interna, donde se toman en cuenta los protocolos y políticas de seguridad será más fácil de administrar y asegurar que aquella enfocada en ofrecer funcionalidad y usabilidad.

Los servicios de Active Directory que se incluyen en el sistema operativo Windows Server es una de las opciones por la que han optado las empresas, para la gestión administrativa de redes informáticas, brindándoles la capacidad de crear servidores de dominio, formar grupos de trabajo y la asignación de privilegios a usuarios. Con la implementación de este servicio muchas empresas han optimizado su desempeño, como la administración de la información, la cual, al estar focalizado en un solo servidor está expuesto a varias amenazas que ponen en riesgo la confidencialidad, la integración y disponibilidad de la información. Partiendo de este punto de seguridad es de vital importancia verificar el nivel de seguridad que se maneja en este tipo de ambiente que en su mayoría de casos de fallos de seguridad es resultado de las malas prácticas de seguridad, que son llevadas desde la implementación, configuración y hasta su aplicación, lo que generan diferentes vulnerabilidades.

El objetivo de este trabajo es enfocarse e identificar las malas prácticas que se generan en este tipo de ambiente de red con el uso de herramientas de intrusión y recomendar un diseño de red que aplique buenas prácticas de seguridad en calidad de políticas y estándares internacionales. Se espera que la presente investigación sirva de guía metodológica para la aplicación de buenas prácticas de seguridad en sistemas informáticos que hagan uso del servicio de Active Directory.

Capítulo I
El Problema

1.1. Planteamiento del Problema

Ubicación del problema

Los sistemas operativos Windows Server ofrecen diversos servicios que gestionan los recursos en una infraestructura de red centralizada, en la actualidad este tipo de administración de redes de ordenadores buscan aprovechar de la mejor forma el crear un dominio de sistema, en el cual la información y seguridad se encuentran organizada en un solo servidor central que brinda un mayor control al administrador de la red.

Desde que Microsoft hace el lanzamiento de este servicio en su sistema operativo Windows Server, las organizaciones encontraran en esta herramienta un modo de gestionar roles y responsabilidades en la red, donde se asignan permisos, usuarios y grupos con el fin de administrar las políticas de la organización. Esto le permite tener una estructura jerárquica que facilite el manejo de información. (Beltrán Ramírez, 2019)

El sistema operativo Windows Server trae consigo el servicio de Directorio Activo, mismo que brinda una infraestructura de red escalable y administración más ágil. Este servicio almacena información de los recursos del dominio y permite el acceso controlado de usuarios y aplicaciones del servidor. La implantación de un servicio de Active Directory permite gestionar los privilegios sobre cada recurso que tengan los usuarios de dominio, esto también permite crear grupos y es posible para un grupo ser parte de otro grupo.

Situación conflicto

Los sistemas de información en las organizaciones o en entornos personales, han tenido un crecimiento directamente proporcional a los avances tecnológicos lo que ha permitido que obtengan ventajas en diferentes aspectos a nivel de sistema, pero a su vez se enfrentan al problema del desconocimiento de protocolos de seguridad que trae consigo incertidumbre en este tipo de ambientes, que los exponen a posibles ataques informáticos que pueden ser físicos o lógicos.

La problemática surge en la credulidad de que manejan la organización en cuanto aspecto de administración de políticas y protocolos de seguridad de la información se refiere. En tal sentido se define que la seguridad de los sistemas no solo depende de la tecnología, sino que también de la correcta administración, un seguimiento riguroso de los procedimientos relacionados con el manejo de información, control en el acceso

físico y auditorias periódicas. Debido a esto el servicio de Directorio Activo se ha convertido en un objetivo para los ciberdelicuentes que buscan comprometer la información de cualquier sistema que presente vulnerabilidades generadas por las mismas empresas o particulares que suelen conformarse con las configuraciones básicas de seguridad. (Beltrán Ramírez, 2019)

Causas y consecuencias del problema

Causas

Así como este servicio brinda la ventaja de administrar recursos de una manera más ágil también representa un punto clave en materia de seguridad informática, debido a que los recursos son administrados en un servidor central convirtiéndolo en un objetivo codiciado por los ciberatacantes, que pueden aprovechar cualquier vulnerabilidad para ingresar a la red de forma física o lógica y una vez se encuentren en ella escalar por la misma hasta llegar al servidor central y obtener información valiosa de la organización.

Debido a su arquitectura jerárquica en la que son asignados a los usuarios mayor privilegio un usuario perteneciente al Active Directory, los errores de seguridad que cometa puede ser más perjudicial para la organización misma. (Casas, 2016)

Las malas prácticas que se generan en este tipo de entornos son más comunes de lo que parece, en la mayoría de casos se deben tipo de privilegios que se les es otorgado a los usuarios del sistema. Existen diversos riesgos de seguridad asociados al acceso de muchos usuarios en una solo red, por eso es vital importancia realizar constante seguimiento a los registros de sesión en el sistema.

El uso incorrecto de credenciales de usuario es una amenaza frecuente, esto se debe a que utilizan contraseñas con datos personales tales como nombre de los hijos, esposo (a), fecha de nacimiento, nombre de la empresa, etc. (Caldas Urduy, 2020)

Utilizar la configuración de grupos por defecto, como el Domain Admin o grupo de administradores, que se encarga de administrar la red interna dándole el privilegio a cualquier usuario de este grupo moverse libremente por la red, donde comúnmente abusan de esta función para asignar privilegios a varios usuarios, utilizando este método como vía rápida en cuanto administración se refiere. (López Jiménez, 2020)

Las vulnerabilidades a las que se exponen comúnmente las organizaciones que usan este servicio se basa en que los privilegios que se les dan a los usuarios pertenecientes al Active Directory van más allá de lo que les corresponden e incluso estas vulnerabilidades de cierta forma las generan los administradores y usuarios con diferentes malas prácticas de seguridad de la información. (Casas, 2016).

Este servicio está basado en los privilegios que se brindan a los usuarios de la red, pertenecientes a uno o varios grupos, de los cuales dependen del conjunto de reglas que controlan el entorno de trabajo proporcionando una gestión centralizada, administrando que pueden y que no pueden hacer en el sistema. Cuando se habla de privilegios se hace énfasis en las vulnerabilidades que se generan por malas prácticas de seguridad en este tipo de entornos, tal como menciona (Holguín Zapata, 2019)En su informe final de práctica empresarial las vulnerabilidades más comunes que se generan en este tipo de entornos son:

- Contraseñas predeterminadas. - Estos errores están asociados al uso de contraseñas predeterminada, que se asocian a hardware y dispositivos de almacenamiento.
- Contraseñas compartidas. - Como principal mecanismo de autenticación en el sistema, por lo que compartirla o dejarla expuesta da paso a que se genere la suplantación de identidad y posterior robo de información.

Consecuencias

La problemática encontrada es el desconocimiento y mala gestión de seguridad a la que se enfrentan las organizaciones que utilizan el servicio de Active Directory, ya que al no aplicar políticas y normas de seguridad informática generan vulnerabilidades que pueden ser explotadas por los malos actores generando pérdidas cuantiosas a la organización, por lo tanto se puede concluir que varias vulnerabilidades son debido al error humano , mismo que puede solucionarse con una guía correcta en administración de seguridad y la definición de políticas y controles de seguridad.

1.2. Formulación del problema

¿Qué herramientas de Pentesting y mitigación de vulnerabilidades ayudarían en el análisis de malas prácticas en Active Directory?

1.3. Delimitación

Área de estudio: Hardware y Redes

Línea de investigación: Redes Inteligentes

Sublímela de investigación: Seguridad

La investigación del presente trabajo está limitado a las malas prácticas de seguridad presentes en los sistemas informáticos que hacen uso de los servicios de Active Directory como parte de su infraestructura de red.

Delimitación espacial

El presente trabajo de titulación será realizado en un entorno virtualizado que permite obtener un ambiente de pruebas controlado y se generen respuestas a las hipótesis que se plantean en base a los sistemas de informáticos que utilizan los servicios de Active Directory.

Delimitación Temporal

La presente investigación será desarrollada dentro de los cinco meses posteriores a la aprobación del tema de titulación.

1.4 Justificación

En el presente trabajo se expondrán las principales vulnerabilidades en las infraestructuras de redes centralizadas que utilicen el servicio de Active Directory generadas por las malas prácticas de seguridad, con el objetivo de brindar un conocimiento del riesgo al que las organizaciones se exponen y brindar un marco de recomendaciones que corrijan dichas vulnerabilidades.

En cuanto a la problemática, se encuentra un problema existente de seguridad en ambientes de infraestructuras de red interna organizacionales que desafortunadamente durante los últimos años han hecho evidente su falta de gestión en políticas y protocolos de seguridad y en efecto se ve reflejado en los múltiples casos de robo información y explotación de brechas de seguridad. Es así como en el análisis y Exposición de vulnerabilidades del servicio de Active Directory que generan las malas prácticas de seguridad con el uso de herramientas de Pentesting y mitigación de vulnerabilidades, serán demostrados los puntos clave que dará a conocer las amenazas que son generadas por un mal régimen de seguridad informática.

En consecuencia, de este mismo contexto se sostiene que si una organización conoce sus riesgos vulnerabilidades y aplica un enfoque de gestión basado en políticas y estándares de seguridad podrá estar más preparada contra incidentes relacionados que comprometan la integridad y confidencialidad de los datos.

Este proyecto busca demostrar los problemas que generan las malas prácticas en este tipo de redes de forma práctica y permita sintetizar ideas que ayuden a mejorar la gestión de seguridad actual en las organizaciones presentando una propuesta de fácil entendimiento para los administradores de Active Directory y a su vez se genere una cultura de buenas prácticas en seguridad de la información en los entornos de red centralizados que utilicen este tipo de servicios.

1.4. Objetivos de la investigación

1.4.1. Objetivo General

Proveer un marco de conocimiento de estándares de seguridad basado en el análisis de vulnerabilidades presentes en redes centralizadas que utilizan el servicio de Active Directory generadas por malas prácticas de seguridad.

1.4.2. Objetivos Específicos

- Identificar la situación actual de la seguridad en los servicios de Active Directory en entornos corporativos.
- Generar un ambiente de pruebas virtualizado que haga uso de los servicios de Active Directory en Windows server y que emule escenarios de malas prácticas de seguridad.
- Ejecutar pruebas de Pentesting en el entorno emulado utilizando herramientas de análisis de vulnerabilidades.
- Definir lineamientos para el desarrollo de políticas de seguridad que reduzcan el nivel de vulnerabilidades en Active Directory.

1.5. Alcance

Análisis de vulnerabilidades que generan las malas prácticas en los sistemas informáticos que utilicen el servicio de Active Directory y desarrollo de lineamientos de políticas de seguridad basado en normas de seguridad de la información que sirva como herramienta para elevar los niveles de seguridad en las organizaciones que hagan uso de este servicio, así mismo se proporciona un marco de seguridad de la información que demuestre los errores de seguridad que cometen ciertos administradores de red durante la implementación y administración de Active Directory.

Los alcances del trabajo de titulación son:

- Realizar una investigación de infraestructura de redes centralizadas y el servicio de Active Directory, utilizando fuentes científicas, libros y páginas web.
- Realizar un diseño de red centralizada con Active Directory en un entorno virtualizado, configurar un escenario de malas prácticas y realizar pruebas con herramientas de pentesting.
- Documentar los resultados de las pruebas de pentesting y realizar un análisis de las vulnerabilidades halladas durante la fase de pruebas.

- Proponer recomendaciones para la definición de políticas de seguridad de la información basado en estándares internacionales de seguridad informática.

Capítulo II

MARCO TEÓRICO

2.1 Antecedentes de investigación

Actualmente en la etapa de globalización tecnológica se incrementa la necesidad de generar un análisis de seguridad que permita evaluar el estado actual de los sistemas informáticos en las distintas organizaciones dando paso a la elaboración de informes que identifiquen los problemas en este tipo de entornos de red. De este modo se utilizan sus resultados para la toma de decisiones y aplicación de nuevas medidas que ayuden a mitigar dichos problemas de seguridad.

Desde el punto de vista de la ciberseguridad Ecuador es uno de los países que más ataques recibe por los hackers, dándole un puesto significativo entre las naciones con mayor incidencia de malware a nivel andino. Según el sitio web (DATTA, 2021) Ecuador ocupa el primer puesto en ataques de tipo ransomware, cuyo método implica el secuestro de datos y su liberación exige un rescate, esto se traduce en el 22% de empresas que sufrieron este tipo de ataque. Durante el periodo de la pandemia la modalidad de teletrabajo trajo consigo el aumento de estos incidentes.

(Deloitte, 2018), realizó un estudio fundamentado en el sondeo de tendencias de riesgos y seguridad de la información en Ecuador, cuyo objetivo era identificar las tendencias de la ciberseguridad en la que se encontraba el país en ese momento.

De esta forma durante su estudio se aplica una metodología basada en la recolección de información a través encuestas donde participaron 84 organizaciones y 5 industrias, siendo ejecutado en un periodo comprendido entre julio y septiembre de 2018. De este modo se obtienen los resultados de las principales tendencias

Tabla 1. *Tendencias de Ciber Riesgos y Seguridad de la Información en Ecuador*

Tendencias identificadas	Resultados
Incidentes de seguridad	4 de cada 10 organizaciones afirman haber sufrido un percance relacionado a la seguridad en los últimos 24 meses y un 70% de las organizaciones no tiene la certeza de la efectividad de respuestas frente a estos incidentes de seguridad.
Presupuesto en ciberseguridad	Se mantiene una tendencia de escases de presupuesto para los oficiales de seguridad de la información (CISO).
Estructura de gobierno de seguridad	Solo 1 de cada 10 organizaciones cuentan con una estructura de seguridad encarga de la gobernanza de ciberseguridad.

Concientización en ciberseguridad	5 de cada 10 organizaciones han puesto en marcha un programa de concientización en ciberseguridad.

Información tomada y adaptada de Informe de Encuestas sobre Tendencias de Ciber Riesgos y Seguridad de la Información en Ecuador. Elaborada por el autor

Frente a la identificación de estas tendencias, con el objetivo de comprobar la situación actual de la ciberseguridad en el Ecuador , (Deloitte, 2020) opta por realizar un estudio basado en una encuesta de sondeo, con preguntas distribuidas por áreas donde participaron alrededor de unas 100 empresas, mismo que se comprende en un periodo de marzo a mayo del año 2020, en ese mismo contexto recientemente en el año 2021 se realiza un segundo sondeo con el fin de actualizar tendencias y estado de la ciberseguridad en el territorio nacional haciendo una comparativa con el estudio previamente realizado, de lo cual se puede resumir en la siguiente tabla.

Tabla 2. *Comparativa del estado actual de la Ciberseguridad en Ecuador.*

Aspectos Claves	Indicadores	Resultados 2020	Resultados 2021
Apoyo de Terceros	Monitoreo de eventos de seguridad	61%	62%
	Gestión de vulnerabilidades	53%	62%
	Monitoreo Antifraude	29%	31%
	Monitoreo y Gestión de incidentes	34%	47%
	Inteligencia de Ciber-amenazas	20%	25%
Anticipación a lo inevitable, herramientas de prevención de riesgos	Herramientas de Backus, Firewalls, Antivirus, Antispam, WAF	16%	22%
Cobertura del Plan de Continuidad de Negocio (BCP)	Amenazas Relacionadas con fenómenos naturales	67%	68%
	Amenazas de Negocio (político, económico, social)	42%	44%
	Amenazas Tecnológicas	71%	86%
	No cuentan con BCP	22%	10%
Dirección Estratégica	Políticas y procedimientos	N/A	72%

	Análisis de Riesgos	N/A	57,3%
	Seguimiento a iniciativas y proyectos	N/A	57,3%
	Aprobación y seguimiento de presupuesto	N/A	53%
	Revisión de auditorías, evaluaciones o diagnósticos	N/A	48,7%
Presupuesto para ciberseguridad	De 25,000 hasta 100,000	40%	32 %
	No cuenta con presupuesto aprobado	25%	39%

Información tomada de Informe de resultados sondeo del Estado Actual de la Ciberseguridad Ecuador 2020 y 2021.Elaborada por el autor

El resultado de ambos estudios revelan aspectos importantes que generan un panorama actualizado de la ciberseguridad en el Ecuador, de tal forma se nota un cambio significativo durante el periodo de sondeo entre uno y el otro estudio dando a entender que pueden mejorar con estrategias orientadas a la supervisión de la administración de ciberseguridad, toma de acciones de aseguramiento, complementación del BCP y un respaldo total a la importancia del presupuesto para implementar las medidas de la dirección de seguridad necesarias.

Por otra parte, la proliferación de ataques cibernéticos a organizaciones ha tenido un aumento significativo en Latinoamérica como afirma (ESET, 2020), que al menos un 60% de ellas reporto haber tenido al menos un percance de seguridad en el año 2019. Colocando al Ecuador con 70% de sus empresas con incidentes de seguridad relacionados infección de código malicioso y ransomware.

Figura 1. *Reporte de Incidentes de Seguridad en empresas de Latinoamérica. Tomado de Reporte de Ciberseguridad LATAM 2020. Elaborado por el autor.*

En relación a esto actualmente el Ecuador se encuentra en el lugar número 82 del Índice Nacional de Seguridad (NCSI) con un 35% como indica (Alvarado Chang, 2020), en su estudio de análisis de ataques cibernéticos hacia Ecuador, clasificándolo como un país de nivel deficiente en ciberseguridad, así mismo se coloca en el puesto 98 del Índice de Ciberseguridad Global con un 37%, 97 en el Índice de desarrollo de las TIC con un 48% y en la posición 82 del Índice de preparación en red con 56% según el mismo (NCSI, 2019)

Figura 2. *Posición en la escala de Índices de Ciberseguridad NCSI- Ecuador. Tomado y adaptado de NCSI. Elaborado por autor*

Tabla 3. *Reporte de Ciberseguridad en Ecuador según NCSI*

Indicadores generales de seguridad cibernética		**Total**
Desarrollo de políticas de seguridad cibernética	0/7 (0 %)	6/27 - (22,22 %)
Análisis e información de amenazas cibernéticas	0/5 (0 %)	
Educación y desarrollo profesional	4/9 (44 %)	
Contribución a la ciberseguridad mundial	2/6 (33 %)	
Indicadores de Ciberseguridad de Línea de Base		7/24 - (29,16 %)
Protección de servicios digitales	1/5 (20 %)	
Protección de servicios esenciales	0/6 (0 %)	
Protección de datos personales	6/9 (67 %)	
Contribución a la ciberseguridad mundial	0/4 (0 %	
Indicadores de Gestión de Incidentes y Crisis		14/26 - (53,84%)
Respuesta a incidentes cibernéticos	5/6 (50 %)	
Gestión de crisis cibernéticas	1/5 (20 %)	
Lucha contra la ciberdelincuencia	4/9 (44 %)	
Operaciones cibernéticas militares	4/6 (67 %)	

Información adaptada de Índice Nacional de Seguridad (NCSI)-Ecuador. Elaborada por el autor

Como se puede inferir en los resultados de estadísticas se proyecta la necesidad de mejorar la calidad de ciberseguridad a nivel organizacional que permita obtener un nivel de desarrollo tecnológico seguro.

Esto apoya la motivación de impulsar propuestas de análisis de seguridad en redes informáticas cuyo recurso más valioso es la información.

(Quevedo Armijos & Sesme Candelario, 2018), realizaron un estudio demostrativo de las distintas vulnerabilidades y riesgos que comprometen los servicios de Active Directory, DNS y DHCP instalados en los sistemas operativos Windows Server 2008, 2012 y 2016 a través de una auditoría de una auditoría de seguridad informática, que tuvo como como objeto la evaluación de estos servicios en diferentes versiones de los servicios de Active Directory haciendo uso de herramientas de test de intrusión que identifiquen las amenazas de este tipo de ambientes y generar un plan de acción para la disminución de las mismas. Posteriormente aplican una metodología basada en la recopilación de información a un grupo de usuarios de la Municipalidad de Guayaquil y profesionales de informática y realizar un análisis estadístico.

Los principales resultados determinan que el 56% de los encuestados consideran los servicios de Windows server más vulnerable que otro tipo y el 70% de los mismo está de acuerdo en realizar auditorías de seguridad en redes de las diferentes áreas que manejan. Por lo tanto, proceden a la aplicación de la propuesta tecnológica evidenciando vulnerabilidades existentes en las estaciones de trabajo de los usuarios que participaron del estudio conforme a esto concluyen que la mayoría de los sistemas evaluados que usan Active Directory son considerados vulnerables por los usuarios ante las amenazas existentes.

La demanda de recursos tecnológicos genera implementaciones de uso prácticos para la centralización de información y administración de usuarios y equipos informáticos. (Ardila Flores & Castro, 2020), en el estudio de verificación del grado de inseguridad de las infraestructuras Windows de directorio activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado, plantearon generar una guía de buenas prácticas mediante la aplicación de pruebas de concepto que permite evaluar la seguridad del servicio de Active Directory en un ambiente simulado.

La metodología que se aplica está basada en diferentes fases, en primer lugar análisis de muestra con elaboración de una encuesta a profesionales y administradores de sistemas que hagan uso de este servicio su respectivos resultados, posteriormente evaluar las malas prácticas de seguridad en un ambiente simulado donde es levantado un servidor de Directorio Activo con característica de inseguridad mismo que es analizado con el uso de herramientas de Pentesting, luego se implementa un nuevo servidor en el mismo entorno simulado con la diferencia que aplica métodos y protocolos de seguridad. Los

resultados de las encuestas reflejan el nivel de Directorio Activos reales, mientras que en el ambiente simulado se evidencia una considerable debilidad de seguridad si se dejan configuraciones predeterminadas. En conclusión, un Directorio Activo requiere un mayor tiempo de administración y control de la plataforma durante la implementación, configuración y gestión por que demanda mayor cantidad de configuraciones.

2.2 Fundamentación Teórica

2.2.1 Redes centralizadas

"Las redes de datos centralizadas son aquellas que mantienen todos los datos en una única computadora, ubicación y para acceder a la información se debe acceder a la computadora principal del sistema, conocida como servidor" (García Perez, 2019)

La administración de red centralizada permite administrar todos los dispositivos conectados a la red desde una sola estación de trabajo o servidor, permitiendo que la tendencia de agregar nuevos dispositivos no suponga un problema para la gestión de procesos de la red. De este modo se pude concluir que la gestión de red centralizada utiliza una comunicación a través de un centro para controlar el acceso de usuarios, almacenamiento de datos y solución de problemas desde su misma estación haciendo uso de una estructura jerárquica donde predominan los privilegios otorgados a los usuarios. (Gallardo Urbini, 2018).

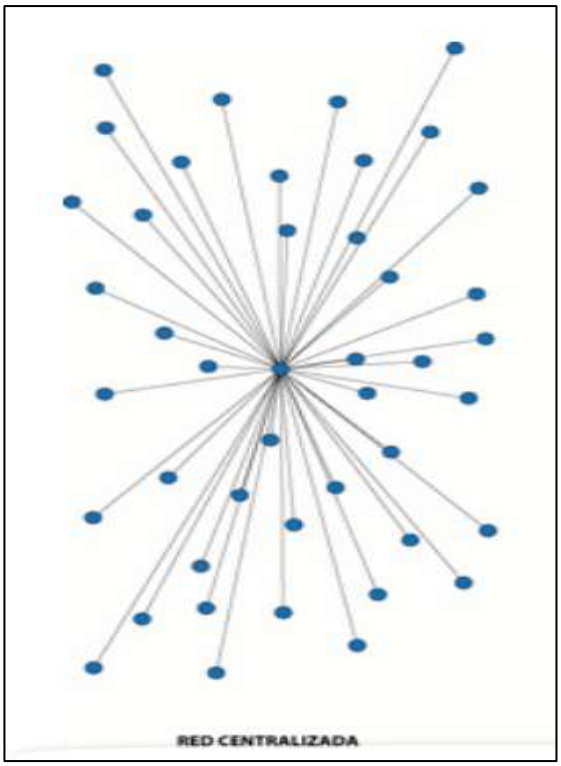


Figura 3. *Red Centralizada. Tomado de www.linkedin.com/pulse/redes-centralizadas-vs-distribuidas-miguel-ángel-pérez-garcía. Elaborador por el autor*

2.2.2 Windows Server

Según SANTOS, 2010. Sistemas Operativos en Red. Madrid: RA_MA editorial, 2010. pág. 23, citado por (Toapanta, 2015) indica que: es un sistema operativo de red que trabaja sobre un modelo denominado dominio, el cual, es un conjunto de equipos (clientes y servidores) que comparten una política de seguridad y una base de datos común (Directorio Activo). Cada dominio debe tener un nombre único.

Windows 2000

Este fue el resultado de la línea para servidores conocida como Windows NT junto a lo que se conoce como la familia Windows 9x cuyos predecesores fueron Windows 95 y Windows 98 que revolucionaron. (Leon, 2019)

De la función de estas dos líneas de desarrollo fue que surgió Windows 2000 profesional para escritorio junto la familia de servidores:

- **Windows 2000 Server:** Para pequeñas empresas o para servidores departamentales de grandes empresas.
- **Windows 2000 Avance Server:** Versión para empresas más grandes con requerimientos de aplicaciones de negocios en línea como soluciones en comercio electrónico y punto.com.

- **Windows 2000 Datacenter Server:** Versión similar a la anterior, aunque con límites más altos en las licencias.
- **Windows 2000 Advanced Server Limited Edition:** Es una versión recortada de la versión Advance Server. (Leon, 2019)

Windows Server 2003

Muchas funciones de la versión de escritorio (XP) se deshabilitaron para ahorrar memoria y mejorar el rendimiento e incorporar los servicios clásicos de Windows Server para orientarlo al mercado de servidores empresariales.

Fue lanzado en varias versiones según su propósito y, a diferencia de las versiones anteriores, no existió una versión de escritorio.

- **Web Edition:** Es la edición especial para montar servicios y alojamiento Web.
- **Standard Edition:** Es la versión de uso general, más apropiada para la mayoría de las empresas pequeñas y medianas.
- **Enterprise Edition:** Es una versión para empresas con mayores requerimientos y que implementa capacidades más amplias que la versión Standard.
- **Datacenter Edition:** Destinada a grandes empresas con requerimientos de procesamiento pesado y grandes volúmenes de datos.
- **Small Business Edition:** Es una versión reducida destinada a empresas con menos de 25 pc. (Leon, 2019)

Windows Server 2008

Agrega nuevas versiones enfocadas principalmente para pequeñas y medianas empresas en un mundo más inter conectados, con mejoras en rendimiento de aplicaciones, gestión de energía y aspectos de seguridad.

Se incluyó el soporte para visualización basado en Hyper-V, el cual supuso un cambio importante en la operativa de los centros de datos permitiendo consolidar servidores de forma más sencilla y transparente.

Esta versión fue lanzada en las siguientes versiones:

- **Windows Server 2008 Standard:** Es la versión de uso general para la mayoría de las empresas pequeñas y medianas.
- **Windows Server 2008 Enterprise:** Destinado a empresas de tamaño medio.

- **Windows Server 2008 Datacenter:** Destinado a grandes empresas con altos requerimientos de procesamiento.
- **Windows Web Server 2008:** Es la edición destinada a la web.
- **Windows Small Business Server 2008:** Destinado a pequeñas empresas.
- **Windows Essential Business Server 2008:** Destinado a empresas medianas.
- **Windows Server 2008 Foundation:** Es una versión destinada a empresas con bajos requerimientos de procesamiento, cantidad de usuarios y hardware reducido.
- **Windows Server 2008 for Itanium-based:** Systems Es una versión especial para procesadores Intel Itanium de arquitectura IA64 que no era compatible con sistemas x86/x86-64. (Leon, 2019)

Windows Server 2012

Este permite instalar una versión llamada Core, que solo proporciona una consola de administración, lo que reduce en gran medida los recursos requeridos o una versión completa con GUI de escritorio.

De igual manera, incorpora un rol de administración de direcciones IP para mejorar la gestión y auditoria de IP en la infraestructura e incorpora, además, para el sistema de ficheros REFS que presenta novedades frente a NTFS, aunque también algunas limitaciones frente a NTFS.

Las ediciones disponibles son las siguientes:

- **Foundation:** Es la versión básica limitada a 15 usuarios, limitado a un CPU y sin soporte para virtualización.
- **Essentials:** Edición para 2 CPU y el límite de usuarios aumenta a 25.
- **Standard:** Hasta 64 procesadores, contiene todas las opciones, únicamente limita a dos máquinas virtuales.
- **Datacenter:** Hasta 64 procesadores, es la versión mayor, contiene todas las opciones, sin límite de instancias virtuales. (Leon, 2019)

Windows Server 2016

Ha incluido mejoras en Active Directory Federation Services, Windows Defender y Remote Desktop Services entre muchas otras.

Desde la reestructura de Microsoft, los equipos de Windows Server y Azure han comenzado a trabajar mucho más de cerca, por lo que han brindado un soporte más maduro para la virtualización en la nube.

- **Windows Server 2016 Essentials** Una versión para menos de 25 usuarios y con varias restricciones con respecto a la versión Standard.
- **Windows Server 2016 Standard** Para entornos físicos o con bajos requerimientos de virtualización.
- **Windows Server 2016 Datacenter:** Para entornos donde la virtualización es vital
- **Windows Server 2016 MultiPoint Premium Server:** Sólo disponible con licencia académica.
- **Windows Storage Server 2016:** Es la versión para almacenamiento dedicado.
- **Microsoft Hyper-V Server 2016**: Es una versión dedicada como Hypervisor. (Leon, 2019)

Windows Server 2019

Esta versión incluye soporte beta para kubernetes además del Windows Subsystem for Linux para obtener una consola bash en Windows que previamente había sido incluida en Windows 10.

Así mismo, permite instalar únicamente una consola prescindiendo de GUI, aunque para la versión con escritorio incluye las mejoras incorporadas en Windows 10.

- **Windows Server 2019 Essentials:** Pequeñas empresas con un máximo de 25 usuarios y 50 dispositivos.
- **Windows Server 2019 Standard**: Para entornos físicos o mínimamente virtualizado.
- **Windows Server 2019 Datacenter:** Entornos de cloud y centros de datos con una gran virtualización. (Leon, 2019)

2.2.3 Directorio Activo o Active Directory

El Directorio Activo es la implementación de Microsoft del servicio de directorios LDAP para ser utilizado en entornos Windows. Permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos computadores, además de almacenar información de una organización en una base de datos centrales, organizados y accesibles. (Gomez, 2010)

Según Olvera y Cesar el Directorio Activo es la herramienta que el dominio utiliza para almacenar información de los usuarios, de los recursos de red, así como información de seguridad importante. Las principales funciones de esta herramienta son agilizar las búsquedas de recursos, usuarios, además de asegurar el proceso de autenticación, optimizando la comunicación entre los equipos de red.

Un Directorio activo no solo contiene la información, sino que también presta los servicios necesarios para poder realizar la administración de esta información desde un único punto.

Por tanto, el Directorio Activo maneja una estructura jerárquica de objetos que se enmarcan en tres grandes categorías, que son: recursos (impresoras), servicios (correos electrónicos) y usuarios (cuentas o grupos).

El Director Activo emplea DNS para la resolución de nombres, proporciona información sobre los objetos, los organiza, controla el acceso y establece la seguridad. Cabe resaltar que separa su estructura lógica que son los bosques, árboles, dominios, unidades organizativas y objetos de la estructura física que son los sitios, controladores de dominios y los servidores de catálogo Global. (Gomez, 2010)

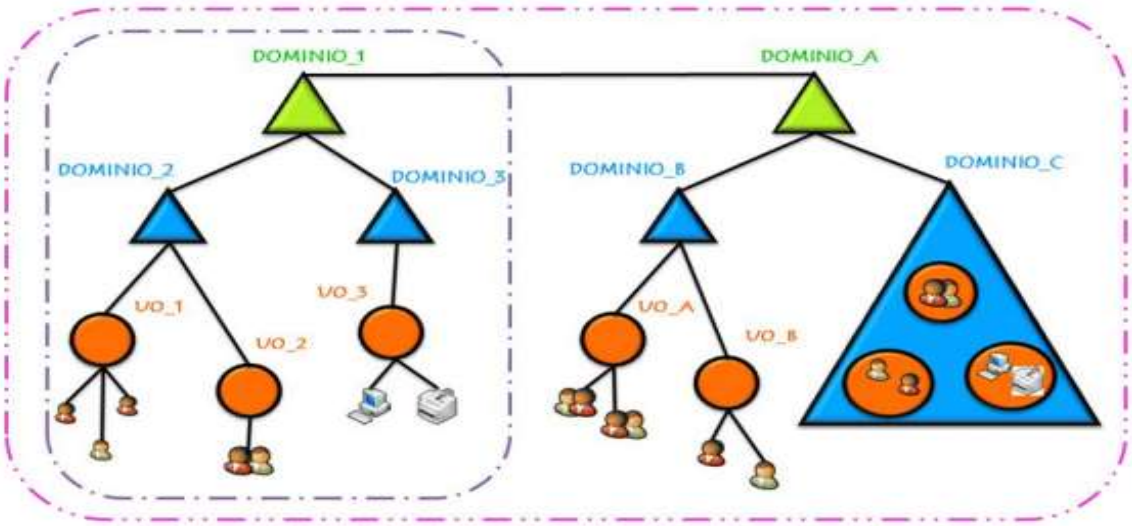


Figura 4 *Estructura de Directorio Activo. Información tomada de la Google. Elaborada por el autor*

2.2.3 Estructura de Lógica de Active Directory

Objetos

Es conocido como la unidad más básica de la estructura lógica, permitiendo la organización de clases con características llamadas atributos. De igual forma estos objetos se definen como esquema o metadatos que existen para poder expandir el esquema o realizar modificaciones cuando ser lo requiera. (Quevedo Armijos & Sesme Candelario, 2018)

Figura 5. *Objetos del Directorio Activo. Tomada de tecnozero.com. Elaborado por el autor.*

Unidades organizativas

Las unidades organizativas (UO - *Organizacional Unir*) son conocidas comúnmente como los contenedores de objetos dentro de un dominio Active Directory. A pesar de que los dominios y bosques se consideren de estructura rígida las UO son más sencillas de diseñar, editar.

Este contenedor incluye objetos como usuarios, contactos, equipos, impresoras, carpetas compartidas e incluso otras UO. De esta manera puede ayudarnos a organizar el almacenamiento de los objetos de un dominio particular del bosque. En este sentido (Jean-François, 2017) se refiere a la capacidad de organización de la UO basado en los siguientes puntos de vista.

- "Desde un punto de vista del contenido, la unidad organizativa puede incluir a los objetos más usados (objetos usuarios, grupos, equipos, carpetas compartidas, impresoras).

- Desde un punto de vista de las funcionalidades de gestión de los cambios en la configuración, la unidad organizativa es el contenedor más pequeño que puede ser objeto de la aplicación de directivas de grupo.
- Desde un punto de vista de la implementación de privilegios de administración, la unidad organizativa puede ser objeto de múltiples delegaciones.
- Desde un punto de vista de la modelización de un espacio organizado, las unidades organizativas pueden ser combinadas de forma sencilla para reflejar su modelo de administración."

Dominios

"El dominio es un componente fundamental de la estructura lógica de Active Directory. Por definición, se trata de un conjunto de objetos de tipo equipo, usuario y otras clases de objetos que comparten una base de datos de directorio común. Estos objetos interactúan con el dominio en función de sus respectivos roles tales como, por ejemplo, los controladores de dominio o simplemente los equipos miembros del citado dominio." (Jean-François, 2017)

De tal forma un dominio puede almacenar objetos relacionados con la finalidad de reflejar la red de la organización, dividendo el directorio principal limitándose a los controladores de dominio en su interior. De hecho, cualquier objeto creado en la red pertenece únicamente a un único dominio por lo que estos representan una limitación de seguridad para el control de accesos a dichos objetos.

Por lo consiguiente brinda funciones tales como:

- Límite de administración a través de reglas del esquema: restricciones y límites de los objetos del dominio.
- Administración de seguridad de los recursos compartidos
- Unidad de replicación para los objetos. (Ferrando Ferrer, 2020)

Arboles

Un árbol es un conjunto de dominios que se encuentra agrupado de forma jerárquica que permite el uso compartido de los recursos globales. En el caso de que se agregue un dominio dentro de un bosque existen dos posibles casos:

- Se genera un dominio hijo en un árbol de dominio existente
- El dominio crea un nuevo árbol de dominio.

A partir de que un nuevo dominio es agregado a uno existente, es considerado un dominio hijo y el existente un dominio padre, no obstante, el hijo puede tener uno o varios dominios hijos, lo que permitirá completar la jerarquía de dominios siendo su base el dominio raíz del árbol. (Jean-François, 2017)

Bosques

Está definido como el mayor contenedor de la estructura lógica de Active Directory por abarcar todos los dominios dentro de un solo ámbito. Estos dominios se encuentran interconectados por relaciones de confianza que se generan automáticamente, creando un vínculo entre bosques que da paso a que los árboles puedan compartir recursos. (Quevedo Armijos & Sesme Candelario, 2018)

Para que un bosque exista es necesario que contenga un Dominio en Active Directory, y a su vez la existencia de cada bosque está bajo el conjunto de controladores de dominio del bosque. Por lo tanto, para tener un bosque operativo es necesario tener un dominio

Instalado. En efecto se concluye que todos los dominios de un bosque comparten de manera común:

- Esquema
- Configuración
- Extensión de búsqueda global a través de los controladores de dominio que actúan como catálogos globales.

Las relaciones. (Jean-François, 2017)

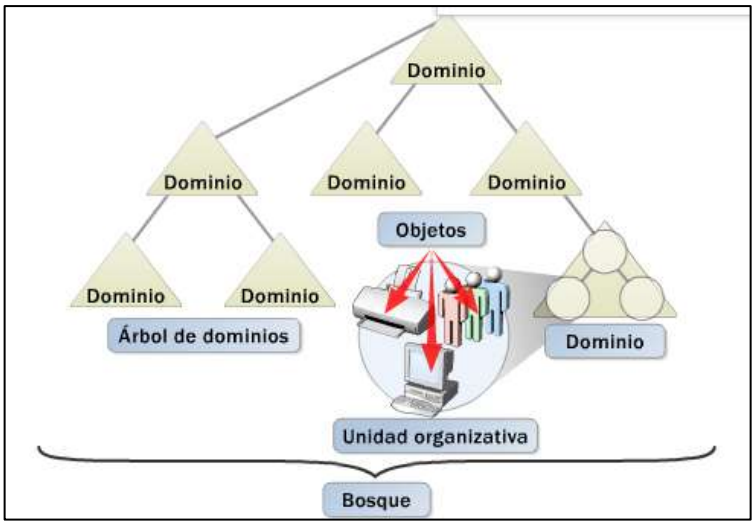


Figura 6. *Estructura Lógica de Active Directory. Información tomada de claretinformaticaasir.blogspot.com. Elaborado por el autor.*

2.2.4 Estructura física de Active Directory

Controlador de dominio

Un controlador de dominio (Domain Controller, DC) es un equipo donde se ejecuta Windows Server y que almacena una réplica del directorio. Los controladores de dominio ejecutan el servicio KDF, que es el responsable de autenticar inicios de sesión de usuarios. (Gomez, 2010)

Gómez (2010), afirma que la información almacenada en cada controlador de dominio se divide en categorías o particiones. Estas particiones del directorio son las unidades de recopilación:

- Partición de directorio de esquema: Contiene todos los tipos de objetos y atributos que pueden ser creados en Active Directory.
- Partición de directorio de configuración: Abarca la estructura de los dominios y la topología de replicación.
- Partición de directorio de dominio: Contiene todos los objetos del directorio para este dominio. Dichos datos se replican a todos los controladores de ese dominio, pero no a otros dominios.
- Partición de directorio de aplicaciones: Estos datos pueden ser de cualquier tipo excepto principales de seguridad (usuarios, grupos y equipos). En este caso, se tiene un control fino sobre el ámbito de la replicación y la ubicación de las réplicas.

Si bien, conforme a estas cuatro particiones de directorio de escritura, existe una cuarta categoría de información almacenada en un controlador de dominio: el catálogo global.

Un servidor de catálogo global es un controlador de dominio que almacena una copia del catálogo y procesa las consultas al mismo. El primer controlador de dominio que se crea en Active Directory es un servidor de catálogo global. Se pueden configurar controladores de dominio adicionales para que sean servidores de catálogo global con el fin de equilibrar el tráfico de autenticación de inicios de sesión y la transferencia de consultas. (Gomez, 2010)

El mismo cumple dos funciones importantes en el directorio:

- Tiene la facultad de permitir que un usuario inicie una sesión en la red mediante el suministro de de la información de pertenencia a grupos universales a un controlador de dominio cuando inicia un proceso de sesión.
- Permite que un usuario busque información de directorio en todo el bosque, independiente de la ubicación de los datos.

Sitios

Los sitios es la agrupación de equipos conectados, que una vez se establecidos los controladores de dominio mantienen una comunicación constante, reduciendo la latencia del sitio. Este tiempo es requerido para el momento que se cree un controlador de dominio y sea replicado, desarrollando una optimización de ancho entre dichos controladores-

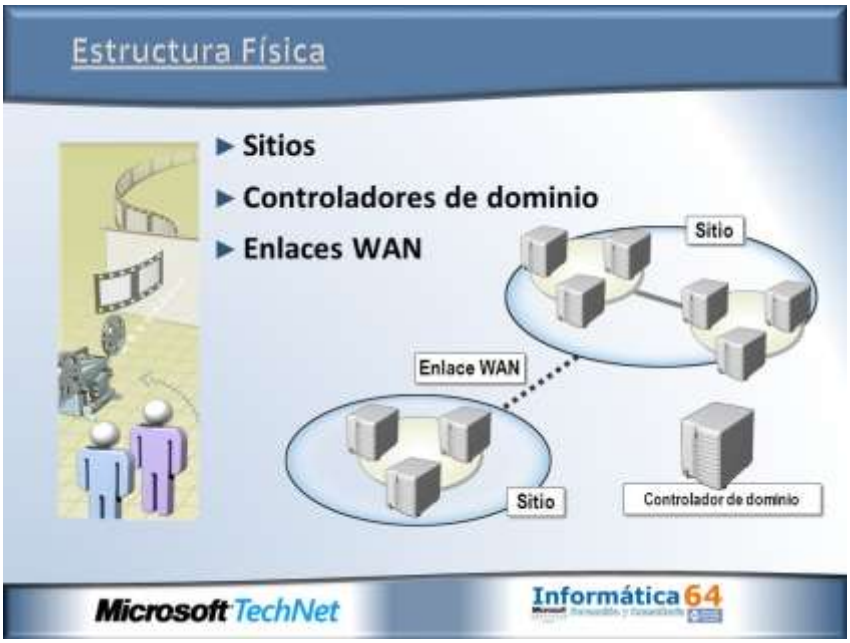


Figura 7. *Estructura Física de Active Directory. Tomado de slideplayer.es. Elaborado por el autor*

2.2.5 Protocolos que utiliza Active Directory

La infraestructura de Windows Server ofrece la capacidad de integrar distintos requisitos para cualquier administrador de red con el objetivo de analizar y compartir información de manera rápida. Este SO hace el uso de varios puertos y protocolos que permiten una comunicación entre su servidor central y los clientes, además de otros servicios de la red como firewalls y demás componentes por lo que para el funcionamiento de este servicio deben estar habilitados lo puertos para TCP y UDP. En este sentido la investigación de (Garcia Guevara, 2015) los protocolos usados por el Directorio Activo son:

Tabla 4 - *Protocolos de Active Directory*

Protocolo	Puerto	Función
LDAP	389	Es un protocolo de nivel de aplicación que brinda el acceso a la búsqueda de información a un servicio de directorio, considerado como la base de datos del Directorio Activo.
DNS	53	Su función es asociar la información con los nombres de dominio asociado a los participantes para que los clientes puedan localizar controladores de dominio y los controladores de dominio que hospedan el servicio de directorio para comunicarse entre sí.
DHCP	67	Permite a los participantes de la red obtener direccionamiento IP automáticamente, funciona como cliente/servidor con una lista de direcciones IP dinámicas para ser asignadas según su requerimiento.
KERBEROS	88	Es el protocolo de autenticación para Directorio Activo, se aplica en redes de ordenadores con la función de autenticar de manera mutua la identidad de los clientes.

Información tomada de la investigación. Elaborada por el autor

2.2.6 Función de Active Directory en la empresa

En la actualidad las empresas han optado por la implementación de los servicios de Active Directory debido a la demanda de administración centralizada de redes que tiene como objeto tener un mayor dominio del sistema de información de la organización con el uso de un repositorio de recursos centralizado.

De la misma forma expresa (Jean-François, 2017) en su libro, que, al unir varios elementos múltiples del sistema, se pueden resolver problemas como la búsqueda de información o el acceso a archivos de manera más eficiente.

Por lo consiguiente significa que Active Directory debe ofrecer los servicios para el almacenamiento de información de cada uno de los objetos de la red y ponerla a

disposición de cada empleado de acuerdo a los permisos y privilegios que son proporcionados.

En definitiva, su función en la empresa es mantener activos los servicios necesarios para la compartición de los recursos para su correcto funcionamiento.

2.2.7 Integración del DNS en Active Directory

En Active Directory la localización de cada uno de sus servicios dependen del DNS (Domain Name System), esto quiere decir que para el correcto funcionamiento del directorio este mismo debe estar siempre disponible.

La configuración adecuada de los servicios DNS garantiza la comunicación entre los controladores de dominio de la infraestructura del directorio activo, esto se expresa en el proceso de inicio de sesión de red o "Net Logon" que permite localizar el controlador de dominio más cercano. (Jean-François, 2017)

Con respecto a esta localización, esta depende de la disponibilidad de la zona misma que se encuentra replicada en los controladores de dominio. En este sentido se establecen la resolución DNS por medio de las peticiones de resolución de registro tipo SRV, utilizados para la localización de servicios, puertos y protocolos, como por ejemplo el servicio de LDAP, autenticación Kerberos y los servicios de catálogo global.

2.2.8 Hardening de sistemas

Todo sistema informático es susceptible a convertirse en objeto de ataques, de tal manera que son constantemente amenazados por diferentes individuos que buscan una oportunidad para obtener lo que deseen. Sim embargo se puede evitar aplicando la metodología de Hardening o endurecimiento de redes.

En cuanto a la seguridad en un entorno informático, "integra sistemas operativos, perfiles de usuarios, activos, control de acceso, políticas de seguridad, infraestructura de distribución y administración de red, métodos de defensa y la concienciación de los usuarios, entre otros componentes." (Huertas Alonso & Tapias Alban, 2016)

El método de protección de un sistema informático que se conforma por elementos lógicos y físicos se denomina Hardening, en tal sentido se termina cuáles son los mejores métodos de seguridad que permitan aislar el sistema de las amenazas.

En este mismo ámbito se menciona en el libro Hacking desde de Daniel Ben chimol que "el proceso de Hardening consiste en ajustar las características propias de un sistema de forma tal que se aumente su nivel de seguridad. Por lo que varios de los ajustes que

suelen incluirse son, deshabilitar servicios y funciones que no se utilicen y reemplazar algunas aplicaciones por versiones más seguras.” (Benchimol, 2011)

Proceso de Hardening

Figura 8. *Proceso de Hardening. . Elaborado por el autor*

Es preciso destacar que, para la obtención de un nivel aceptable de endurecimiento del sistema, es necesario tener en cuenta varios aspectos tales como técnicos y humanos. De Este modo se concluye que este método se debe utilizar de forma preventiva y en conjunto con la aplicación de la defensa profunda. (Robaypo López & Rodríguez Rodríguez, 2015,)

Hardening de Active Directory

Para el endurecimiento de los servicios de AD es necesario aplicar buenas prácticas de seguridad y administración que brinde un mayor control y aseguré el perímetro de nuestro sistema informático en base al cumplimiento de políticas de seguridad.

Frente a esto se encuentran estas recomendaciones:

- Restricción de portal administrativo
- Bloque de ubicaciones y rangos de IP desconocidos
- Aplicación de parches de seguridad
- Protección y supervisión de cuentas privilegiadas
- Eliminación de membresías en grupos de alto privilegio
- Implementación de host administrativos seguros

- Aplicar listas de permisos a las aplicaciones
- Aislación de sistemas heredados
- Utilización de firewalls
- Migre los activos críticos a bosques con mayores requisitos de seguridad (Microsoft, 2018)

2.2.9 Técnicas de Pentesting

Existen diferentes tipos de pentesting que se clasifican de acuerdo al conocimiento o información que se le brinda para las pruebas.

- **Prueba de caja Negra o Black-Box. -** En este tipo el tester no tiene información anticipada sobre la red o su sistema informático, solo cuenta con herramientas propias y se le brinda una dirección ir de algún sitio con el objetivo que actué como hacker malicioso.
- **Prueba de caja blanca o White-Box**. **-** Se cuenta con el acceso autorizado a toda la información de redes, servidores, equipos finales y demás que componen la organización, de este modo evalúa la seguridad de los equipos.
- **Prueba de caja gris o Grey-Box. -** el escenario en que se desarrolla esta prueba es con información parcial de la empresa, donde se emulan un ataque de personal interno de la empresa como un empleado inconforme. (Barreto Cuitiva, 2018)

De las técnicas identificadas se elige las pruebas de caja blanca o White Box, por el hecho de que el análisis está enfocado a un ambiente implementado y emulación de un escenario de autorización por parte de la organización, con el objeto de verificar el grado de inseguridad que mantienen en los sistemas informáticos que hagan uso de los servicios de Active Directory.

2.2.10 Fases de pentesting y herramientas de pentesting

Para llevar a cabo un test de intrusión exitoso es necesario atravesar por varias fases que permitan determinar el nivel de seguridad del sistema que se está probando. Como indican (Huertas Alonso & Tapias Alban, 2016) que este tipo de pruebas utilizan ataques pasivos por qué no involucra cambios en el sistema y en efecto analizar solo la red y los servicios de la misma.

***Tabla 5**. Fase de Pentesting White Box*

Fase	Descripción
Reconocimiento	Es la etapa que toma más tiempo, porque se busca definir al objetivo, su información para tener un plan de ataque.
Escaneo	Hace uso de la información previa para la detección de puntos vitales de la organización, empezando por puertos abierto, posteriormente se asocian a un servicio del atacante para encontrar vulnerabilidades
Enumeración	Se busca obtener información relevante de usuarios, equipos, red y otros recursos.
Acceso	Después de haber encontrado las vulnerabilidades, el acceso al sistema toma prioridad y se procede a realizar la explotación de estas.
Mantenimiento de acceso	Tiene como objeto mantener una sesión activa entre el equipo comprometido y el atacante. Para ello se utilizan métodos y herramientas que hagan perdurar dicho acceso como software malicioso.

Información tomada de investigación directa. Elaborada por el autor

2.2.11 Herramientas para la identificación de vulnerabilidades

***Tabla 6.** Análisis comparativo de herramientas de pentesting.*

Fase	Herramientas	Características
Reconocimiento	DNSdumpster	• Descubre subdominios relacionados con el dominio de destino. • Tiene un límite en la cantidad que puede buscar • Se ejecuta desde el navegador • gratuito

	Sonda	• Tiene un motor de búsqueda de ciberseguridad. • Se ejecuta desde el navegador
	Maltego	• Muestra la exposición del servidor en internet • Coteja información perfiles en redes sociales, servidores de correo, etc. • Muestra los datos de forma gráfica. • Requiere instalación
	Informe Rsop.msc	• Genera informes sobre las directivas de grupo aplicadas a un usuario o a un equipo de Windows. • vista gráfica o una vista de línea de comandos • formato estándar abierto para la búsqueda, scripts, etc. • Ejecución desde el equipo perteneciente al dominio
	Gpresult/R	• Se ejecuta desde cmd • Muestra la configuración de las directivas de grupo del equipo e información de la cuenta de usuario
Escaneo	Nmap	• Identificación de servidores en la red local y a través de internet. • Ejecución por consola • Identificación de puertos abiertos y los servicios que ejecutan • Gratuita y de código abierto • Escaneos programados
	Nessus	• Escanea vulnerabilidades en la red local • Gratuito y de paga • Ejecución por consola e interfaz grafica • Base de datos de vulnerabilidades • Reporte de vulnerabilidades y su nivel de riesgo • Escaneos programados • Requiere instalación y registro de cuenta

	Wireshark	• Robusto • Captura paquetes de datos de la red o almacenados en un archivo • Interfaz flexible • Genera estadísticas
	OpenVas	• Gratuito y de código abierto • Documentación extensa • Reporte de vulnerabilidades y su nivel de riesgo • Ejecución por línea de comandos o de forma grafica • Servidor web integrado • Requiere instalación
	OWASP	• Escaneo de servidores web • Gratuito y código abierto • Requiere instalación y tener java 7 o superior instalado • Documentación extensa •
Enumeración	DNSenum	• Script en Perl • Enumera la información de DNS del dominio • fuerza bruta a los subdominios
	Nmap	• De código abierto • Identifica subdominios adjuntos a un dominio especifico • Funciona solo bajo Linux • Busca servidores mal configurados y / o sin parche.
	Nbtscan	• Busca servidores de nombres NETBIOS abiertos en una red TCP / IP local o remota • No necesita instalación • Descubre direcciones MAC y clientes del dominio
	Enum4linux	• Extrae información del servidor • Recupera información de políticas de contraseña, RDIP, dominio y usuarios.

Información tomada de investigación directa. Elaborada por el autor.

Herramientas seleccionadas para cada fase

Después de la revisión de las características de las herramientas utilizadas en cada fase se eligen las siguientes, mismas que se eligen por sus facilidades de uso y funciones hará la evaluación de vulnerabilidades para el escenario planteado de pentesting de caja blanca a un directorio activo con malas prácticas de seguridad.

Tabla 7. *Herramientas seleccionadas para pruebas de pentesting.*

Fase	Herramientas
Reconocimiento	• informe Rsop.msc • Entusar • Gpresult/R
Escaneo	• Nmap • Nessus • OpenVas
Enumeración	• Nbtscan • Enum4linux

Información tomada de investigación directa. Elaborada por el autor.

2.2.12 Vulnerabilidades de seguridad en la administración de active Directory

Los entornos de Active Directory tienen vulnerabilidades que ponen en riesgo la seguridad del mismo, de forma que pueden afectaren en poca o mayor medida a la organización. La razón de ello se debe a que una sola vulnerabilidad puede dar paso a que una amenaza se materialice con graves consecuencias, es así como el caso de que una vulnerabilidad de acceso le permita a un atacante ingresar y obtener información de la empresa. En el mismo sentido se presentan las vulnerabilidades más comunes que se generan en estos ambientes por una incorrecta administración de los servicios de Active Directory.

Vulnerabilidad del protocolo NetLogong

Esta vulnerabilidad que ha sido detectada y nombrada como Zerologon, le permite a un atacante una explotación exitosa de los servicios de AD para tomar el control de la red a través de una aplicación desarrollada especialmente con esta finalidad en cualquier dispositivo de la red. (INCIBE, 2020)

CVE-2011-2014: Se ha descubierto una vulnerabilidad en "Active Directory" en Windows. La vulnerabilidad reside en un error al utilizar "LDAP" sobre "SSL"

Un atacante remoto podría obtener acceso y aumentar sus privilegios mediante un certificado que ha sido revocado especialmente manipulado.

CVE-2009-2508: La vulnerabilidad reside en un error en la implementación de autenticación el cual no borra convenientemente las credenciales al final de una sesión de red. Un atacante remoto podría obtener las credenciales de un usuario mediante la caché del mismo navegador.

Puerto 445 abierto: Es una de las vulnerabilidades más comunes que se encuentran es que las empresas dejan el puerto 445 abierto por una configuración inadecuada, este puerto sirve para la ejecución de los servicios de Active Directory, lo cual representa un riesgo que puede ser materializado en una explotación de credenciales de usuario para tener acceso al dominio de la empresa. (Quevedo Armijos & Sesme Candelario, 2018)

2.2.13 Políticas de seguridad de la información

La política de seguridad de la información se define como una guía para la toma de decisiones, los gerentes enfrentan decisiones difíciles con respecto a la asignación de recursos, objetivos en competencia y estrategia organizacional, todos los cuales se relacionan con la protección técnica y recursos de información, así como orientar el comportamiento de los empleados. Los gerentes de todos los niveles toman decisiones que pueden afectar la política, con el alcance de la aplicabilidad de la política que varían según el alcance de la autoridad del gerente

Las políticas de seguridad se desarrollan como medida de protección para la diversidad de amenazas internas y externas a las que es sometida la información, en búsqueda de la reducción de los riesgos, cuyo éxito se basa en el compromiso de los que estén a cargo, la difusión y de igual forma del compromiso de los usuarios de aplicar en su totalidad dichas políticas. (Torres Núñez, 2015)

Mediante las políticas de seguridad se establecen las normas de tratamiento y actuación del personal, relacionado a los recursos y servicios informáticos importantes de la institución. Cuyo fin es que se cumplan las mismas y de caso contrario se deben aplicar los correctivos correspondientes, asimismo estas estarán orientadas a las decisiones de seguridad, lo que requiere la disposición de cada uno de los miembros de la organización para lograr la visión planteada. (Arias Villafuerte & Isabel, 2015)

2.2.13.1 Normas y estándares de seguridad de la información

Normas ISO

Se conocen como las normas ISO a todo documento que por lo general específica requerimientos que son empleados o destinados a las organizaciones con el fin de otorgar y permitir que los productos o servicios puedan tener un orden en cuanto a cumplimiento, el cual es evaluado por diferentes organizaciones o entes reguladores con el fin de verificar garantizar su integridad.

Actualmente ISO por sus siglas en inglés de (International Organización for Organización) al día de hoy tiene publicado más de 19.000 normas internacionales que pueden ser obtenidas desde el sitio oficial.

Funcionalidad de las Normas ISO

Las normas ISO como se mencionó con anterioridad tienen como fin asegurar que todos los productos o servicios cuenten con las características deseadas para ello se basa a diferentes instrumentos favoreciendo la productividad con beneficios tales como:

- Permite el acceso a nuevos mercados
- Evaluar tecnologías acordes a estándares de funcionamiento
- Extensa información para aplicación de normas

ISO 27001

ISO 27001 es una normativa de carácter internacional que permite garantizar la TRIA de la seguridad informática basada en la Confidencialidad, Integridad y Disponibilidad de la información que existe en todo sistema, así como la forma en como son procesados en los sistemas de TI.

Por lo general ISO 27001:2013 permite a las instituciones poder evaluar los riesgos, así como la aplicación mediante controles necesarios que pueden ayudar a controlar, eliminar o aceptar el problema actual.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización que cumple con las fases necesarias en cuanto a diseño y buenas prácticas establecidos en ISO.

Esta normativa se centra en la protección de los tres aspectos fundamentales de seguridad de la información, la confidencialidad, integridad y disponibilidad de la información, aplicando métodos y controles de evacuación, mitigación y tratamiento del riesgo. (Acosta Herran, 2018)

Ventajas de implementar ISO 27001

- Mejora en los controles de seguridad en cuanto a coordinación y funcionamiento
- Integración de metodologías que permitan la reducción de riesgos y mejorar en cuanto al nivel de seguridad
- Favorecimiento en cuanto a normativas legales requeridos por entes de control.
- Mayor valor en el mercado y confianza acorde a procesos de TI al tener certificación
- Reducción de costos en cuanto a eficiencia que se emplee

Cobit 5

COBIT 5 por sus siglas en español (Objetivos de Control para las Tecnologías de la Información y Relacionadas) es un frame de trabajo que tiene como fin permitir dar a conocer la aplicación de los entes gubernamentales al igual que las tecnologías de la información que son aplicados a una institución en sí con ello se busca evaluar el estado en el que actualmente se encuentra la empresa en cuanto a TI mediante ciertos criterios de evaluación.

Cobit tiene 5 principios que una empresa debe seguir si desean adoptar una mejor gestión en cuanto TI las cuales se detallan a continuación:

- La satisfacción que existen por parte de los accionistas
- Tener consideraciones en cuanto a tecnología desde el principio a fin de cada empresa
- Aplicación de un modelo de referencia integrado
- Permitir un enfoque holístico
- Identificar y dividir al gobierno de la gestión

Instituto Nacional de Estándares y Tecnología Publicación Especial 800- 12. (NIST 800-12)

Es una serie de publicaciones de documentos de investigación que describe ´políticas de seguridad de la información, procedimientos y directrices, por lo que brinda información relacionada la gestión de proceso de gestión de seguridad de la información. Con respecto a la NIST 800-12, como parte de la serie SP muestra de manera general un enfoque de controles operativos y técnicos enmarcados en el ciclo de vida del SGSI que contempla las fases de:

- Iniciación,
- Desarrollo
- Adquisición

- Implementación
- Operación
- Mantenimiento y disposición. (Salamanca, 2016)

2.3 Bases Conceptuales

- **Active Directory**

Una de las herramientas que se utiliza para organizar y gestionar los recursos de una red computadoras y todo lo que a ello implica (usuarios, servicios, grupos, servidores, dominios, permisos) es el Active Directory (Directorio Activo). Este es un servicio que le permite a los administradores de red establecer políticas de seguridad en toda la red, desplegar programas en muchas computadoras y almacenar la información de forma centralizada, organizada y accesible (Maité Martínez González, 2018)

- **Ciberseguridad**

Se entiende por ciberseguridad como la protección de activos de información, mediante el tratamiento de las amenazas. Con el uso de las Tecnologías de la Información y la comunicación, se facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, que conlleva serios riesgos y amenazas en un mundo globalizado; y las amenazas en el espacio digital adquieren una dimensión global que va más allá de la tecnología. (Fernández Bermejo & Martínez Atienza, 2018)

- **Pruebas White box**

Es el tipo de prueba que realiza un tester al cual se la ha brindado la información pertinente sobre sistemas, la red, esquemas y detalles de sistemas operativos, de esta forma el pentester evalúa de forma crítica y sin mayor esfuerzo las vulnerabilidades de seguridad, enfocado a eliminar los problemas de seguridad interna. (López de Jiménez, 2017)

- **Hacker**

Es una persona o a una comunidad que posee conocimientos en el área de informática y se dedica a acceder a sistemas informáticos para realizar modificaciones en el mismo.

- **Vulnerabilidad**

La vulnerabilidad son los fallos de los sistemas de seguridad o en los propios que el usuario utiliza para desarrollar las actividades que permitirían que una

amenaza tuviera éxito a la hora de generar un problema. (Romero Castro, y otros, 2018)

- **Amenaza**

Las amenazas son eventos accidentales o intencionados que puede ocasionar algún daño al sistema informático y ocasionar pérdidas materiales o financieras o de otro tipo. Existen diferentes tipos de amenazas; naturales (incendios, inundación, tormenta, fallas eléctricas, explosiones, etc.); agentes externos (ataques de una organización criminal, sabotajes, disturbios y conflictos sociales, robos, estafas, virus informáticos, etc.); y agentes internos (descuidos del personal, errores involuntarios en el manejo de herramientas, sabotaje por parte de empleados descontentos, entre otras). (Sain, 2018)

- **Seguridad**

Como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad. (Romero Castro, y otros, 2018)

La seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como información, hardware o software. (Gil Vera & Gil Vera, 2017)

- **Ingeniería social**

Puede definirse como una acción o conducta social destinada a conseguir información de las personas cercanas a un sistema. Es el arte de conseguir de un tercero aquellos datos de interés para el atacante por medio de habilidades sociales. Estas prácticas están relacionadas con la comunicación entre seres humanos. (Cristian Brochillo, 2009)

Es un ataque cibernético en el cual se obtiene datos confidenciales a través de la manipulación a la víctima mediante técnicas de persuasión y engaño, es una de las herramientas más utilizadas por los caber- delincuentes, ya que a través del tiempo debido a la evolución tecnológica se ha ido mejorando e incrementando el robo de información. (Tamayo Argoti, 2020)

- **Pentesting**

Se empieza con el escaneo, identificación y análisis de vulnerabilidades de un sistema remoto, luego sigue la creación de un exploit que posibilita tomar ventaja

de una vulnerabilidad para acceder a dicho sistema, sobre el cual se examinan las posibles acciones de post-explotación que se pueden realizar para intentar tomar control del sistema; y, finalmente se ofrece un conjunto de medidas que ayuden a mitigar los problemas de seguridad detectados. (Pastor Ricós, 2020)

- **Virtualización**

Es la tecnología que permite la emulación un sistema informático mediante software, reemplazando a uno físico, donde incluye versiones de hardware, sistemas operativos, dispositivos de almacenamiento, tarjetas y entre otros componentes que emulan a los físicos (Domínguez Sanjuán, 2018) . De tal forma que brinda la posibilidad de tener en un solo equipo varios computadores virtuales, particionado los recursos de este, donde cada máquina virtual actúa de forma independiente ejecutando sistemas operativos y programas al mismo tiempo en un solo host físico.

- **Máquina virtual**

Una máquina virtual (VM) es una emulación de un sistema informático. Estas están basadas en la arquitectura de las computadoras físicas, con la diferencia que se ejecutan a nivel lógico, sus implementaciones pueden involucrar hardware especializado, software o una combinación. (Domínguez Sanjuán, 2018)

- **Malas practicas**

Son aquellas prácticas en las que por desconocimiento, torpeza o inexperiencia se generan efectos negativos que afecten la continuidad de un proceso ya sea en baja o alta escala.

Capitulo III

La propuesta

3.1. Diseño de la investigación

3.1.1. Investigación descriptiva

Es un método cuantitativo utilizado para la evaluación de una determinada problemática, que incluya las características de una población o situación particular, puntualizando las características más fundamentales de estas generando información sistemática comparable a otras fuentes. Debido a esto la información proporcionada debe ser de carácter precisa, donde esta debe ser fundamentada en características visibles y comprobables

El objetivo de este tipo de investigación es dar a conocer situaciones, costumbres comportamientos a través de la descripción de actividades, objetos, procesos y personas (Guevara Alban, Verdesoto Arguello, & Castro Molina, 2020)

El uso de esta metodología será de ayuda dentro del presente trabajo para describir de manera sistemática y analítica la problemática de la investigación y poder identificar las características y extraer datos cualitativos de los métodos de recolección de información y los casos de estudio durante el desarrollo de la propuesta.

3.2. Métodos de recolección de información

3.2.1. Investigación Documental o bibliográfica

La investigación documental permite aplicar métodos de recolección información de distintos tipos de fuentes escritas o audiovisuales, dando paso a la extracción de datos relevantes respecto a la investigación haciendo uso de medios tales como uso de libros, revistas de investigación, enciclopedias temáticas, documentos escritos, grabados o digitalizados, etc. (Reyes Romero, Mejía Sáenz, & Sánchez Carlessi, 2018)

Dentro del desarrollo de la investigación realizada se ha hecho uso de este método para sentar las bases teóricas en fuentes científicas en concordancia con investigaciones anteriores que enfaticen el tema de seguridad en redes empresariales y las malas prácticas que se generan en entornos de red centralizados.

3.2.2. La entrevista

La entrevista se considera una técnica de recolección de información utilizada en el proceso de investigación, donde esta tiene el mismo valor si se da en el desarrollo de una investigación, así como en un estudio sistematizado, teniendo las mismas características y pasos de cualquier otro método de recolección de información. (Folgueiras Bertomeu, 2016)

Después de definir las preguntas, se entrevistó al Ingeniero Byron Zambrano, administrador de red y sistemas del centro médico MediLink en la ciudad de Guayaquil, como profesional a cargo del área de sistemas con el objetivo de obtener la perspectiva de un experto en administración de redes internas y obtener información adicional sobre los aspectos de la seguridad de Active Directory a nivel empresarial que contribuya a identificar factores que contribuyen a al desarrollo de la inseguridad en Active Directory.

1. ¿Qué opina sobre la ciberseguridad a nivel de redes internas?

Respuesta. - Es un tema necesario y en nuestro entorno no le dan la prioridad que se merece, por ende, las empresas tienen demasiadas vulnerabilidades a nivel informático

Análisis e interpretación. - El punto de vista del entrevistado refleja su preocupación por el bajo nivel de importancia que las empresas le dan a la ciberseguridad, dado que este factor debe formar parte primordial en la administración de las empresas, lo que concuerda con ciertos antecedentes de la importancia que le dan las empresas a la ciberseguridad.

2. ¿Cómo calificaría el grado de seguridad que tiene actualmente los servicios de Active Directory en su organización del 1 al 10? Siendo 1 más inseguro y 10 muy seguro.

Respuesta. - Lo calificaría como un 7, ya que existen varios puntos por mejorar de acuerdo a la seguridad.

Análisis e interpretación. - Un grado de seguridad moderado no es suficiente por lo que ciertamente se es necesario implementar mejoras con el fin de llevarlo al máximo, aplicando los correctivos necesarios en redes existentes y metodologías para las que se prevén implementar.

3. ¿Tiene conocimiento si la configuración de los servicios de Active Directory en su organización se hicieron en base a estándares o metodologías de seguridad?

Respuesta. - Están hechas en base a una metodología de seguridad, pero no en una en específico, sino que utilizando métodos de varias como la ISO 2700 entre otras.

Análisis. - Definitivamente debe ser de importancia que la implementación de un sistema informático está basada en metodologías o estándares internacionales certificados que permitan garantizar seguridad del sistema y los servicios que forman parte de e.

4. ¿Cómo cree usted que la administración de los servicios de Active Directory mejorarían si conociera las vulnerabilidades de seguridad que tiene? Respuesta. - Debería disminuir el grado de inseguridad, pero la seguridad informática no solo es a nivel tecnológico, también es un tema social por lo cual los usuarios deben ser capacitados en estos temas.

Análisis. - La administración de un sistema informático de servidores no solo demanda un conocimiento tecnológico del administrador sino también de los usuarios puesto que al final estos son los que acceden e ingresan la información al sistema por lo tanto generar un ambiente de conciencia social sobre seguridad informática es fundamental a la hora de aplicar medidas de reducción de vulnerabilidades.

5. ¿Qué factores cree que influyen al momento de determinar si un sistema es seguro o inseguro?

Respuesta. – En referencia a factores de configuración serían los protocolos de conexión, autenticación, cifrado de la información, sin embargo, la influencia del factor humano es importante respecto a la administración.

Análisis. - Es claro que las configuraciones de un sistema son determinantes al momento de determinar su seguridad y así mismo lo es el usurario del sistema ya que de este depende en cierta medida la aplicación de las configuraciones y seguir medidas de seguridad para mantener al sistema como seguro.

6. ¿Cuáles son los métodos que aplica para mantener la seguridad en los servicios de Active Directory?

Respuesta. - Principalmente socializar con los usuarios sobre ataques como phishing y políticas de contraseñas, no compartir sus credenciales de usuarios y no utilizar dispositivos de almacenamiento externo sin autorización.

Análisis. - La aplicación de métodos de conciencia social sobre los distintos riesgos y amenazas informáticas, podrían generar beneficios que complementen otras medidas de seguridad, lo que daría paso a la mitigación de vulnerabilidades.

7. **¿Si tuviera a su disposición una guía de políticas y buenas prácticas de seguridad en Active Directory, podría mejorar su administración?**

Respuesta. - Seguro que se podría mejorar y complementar los servicios actuales, ya que a veces la información que se encuentra en internet no es muy clara.

Análisis. - Actualmente existe información sobre buenas prácticas de seguridad y políticas de seguridad en los servicios de Active Directory, pero a su vez esta se encuentra dispersa o no es tan concreta y respecto a malas prácticas es escasa. Por lo tanto, se hace necesario recabar y sintetizar información de utilidad, que sirva de guía práctica para administradores y usuarios de Active Directory.

3.3. Situación actual de la seguridad en redes centralizadas

3.3.1. Seguridad de Active Directory en la empresa

Una correcta dirección de la seguridad en el servicio de Active Directory de Windows Server contribuye a la buena operativa de los sistemas de información. De tal manera es considerado como la primera capa de seguridad en cuanto nivel de red empresarial se trata.

La gestión de seguridad está basada en los roles de seguridad que establecen las directivas de grupo.

Los componentes encargados de la seguridad son:

- Las listas de control de acceso ACL, se encargan de los permisos de los objetos.
- Las entradas de control de acceso ACE, establecen los directores y permisos de seguridad.

El control de acceso a la red está controlado por las políticas de grupo que regulan el acceso a los recursos de la red, que permite la adaptabilidad por usuario. Estas políticas están definidas como:

Configuración de equipos. - especifica los procedimientos del sistema operativo, como apariencia, aplicaciones, seguridad y scripts programables.

Configuración de usuarios. - se determina accesos de usuarios a panel de control, configuraciones de red, de sistema, internet e instalación de software, esta configuración está disponible una vez el usuario inicia sesión en su estación de trabajo. (Ferrando Ferrer, 2020)

En la actualidad alrededor de un 90% de las empresas han implementado los servicios de Active Directory como herramienta de gestión y autenticación de usuario, esto lo pone en la mira de los malos actores como un objetivo de penetración para obtener información de las organizaciones, de tal forma que su protección demanda recursos de análisis y monitoreo que ayuden a detectar las falencias en sus sistemas, colocándolo en una situación complicada respecto a la seguridad.

Es así que los cibercriminales han tomado ventaja, siendo que un 80% de los ataques empresariales involucra a los servicios de Active Directory de naturaleza de abuso de acceso privilegiado, donde el común denominador de la mayoría de estos ataques es las fallas de configuración de este, dando como resultado fugas de datos. (Vázquez, 2021)

En el mismo contexto (Vázquez, 2021), menciona que existe una preocupación en las empresas, especialmente en los responsables de la seguridad digital empresarial, esto se destaca en el estudio a los líderes de ciberseguridad donde se obtuvieron resultados tales como:

- 97% de las organizaciones considera a Active Directory como elemento critico
- 47% de las organizaciones utiliza los servicios de Active Directory como fuente de almacenamiento de credenciales.
- 64% afirma que en caso de la caída de Active Directory sufrirían consecuencias catastróficas para su compañía.
- +50% de las empresas no tiene un plan de continuidad de negocio que contemple recuperar los servicios de Active Directory en caso de pérdidas.

3.3.2. Malas prácticas de seguridad más comunes en active Directory

- **Configuraciones por defecto. -** En la instalación de los servicios de Active Directory, existen configuraciones de seguridad por defecto que no contemplan escenarios de inseguridad para el correcto funcionamiento del mismo, sin embargo, a pesar de esto las empresas que implementan estos servicios hacen caso omiso a una correcta guía de configuración y utilizan dicha configuración por defecto que puede descaderar en problemas y vulnerabilidades que expongan a la organización.
- **Permisos excesivos a grupos o usuarios. -** Este error de administración se relaciona al buscar una simplicidad de permisos en la red a los usuarios, lo que podría terminar en un desastre. Es así que cualquier usuario que tenga más permisos de los necesarios, tales como ver, modificar, eliminar información no relacionada a su estación de trabajo, conlleva a consecuencias como perdida de datos, violaciones de seguridad o modificación incorrecta de archivos.
- **Asignación incorrecta de membresía de grupos. -** Debido a que los grupos cuentas con membresías para comunicarse con otros, sean estos de nivel inferior o superior, al agregarse un nuevo miembro al grupo se agregan indirectamente a otro por el mismo hecho de que el grupo al que pertenecen esta anidado a otro. Debido a esto se puede generar un conflicto de permisibilidad a un grupo al que el usuario no debería tener acceso.
- **No depurar cuentas obsoletas. -** Esta mala práctica se genera una vez que un empleado abandona la organización y su cuenta de usuario no es depurada del servidor, siendo que en el caso de no hacerlo los malos actores utilizando herramientas especializadas aprovechan esta vulnerabilidad para acceder a la información de la empresa, así mismo las licencias que utilizaba ese usuario deben ser reasignadas. (Manageengine, 2019)
- **Cuen tas de servicio configurado como administradores de dominio. -** Es común ver que en las organizaciones las cuentas de servicios se le asignan permisos de AD para que este pueda ejecutarse sin problemas dentro del entorno de sistemas. Sim embargo otorgar

estos permisos puede resultar ser dañino debido que los privilegios de administrador de dominio permiten autenticar e identificar una cuenta como servicio, iniciar o ejecutar código o una aplicación, o iniciar un proceso.

- **Problemas de política de contraseñas y debilidad de cifrado. -** Las políticas de contraseñas que se configuren con un bajo nivel de seguridad y que estas no tengan caducidad generan vulnerabilidades a nivel de acceso con el riesgo de ser descifradas fácilmente por ajenos a la organización. En el mismo sentido la encriptación que se maneja juega un papel importante, es así como es recomendable el uso del algoritmo LM y evitar el reciclado de contraseñas en las cuentas de servicio. (BrandPost, 2021)
- **Planes de recuperación/copias de seguridad deficientes. -** Tener un plan para respaldar la información de la empresa es nefario en la gestión de los servicios de Directorio Activo, pero a su vez las organizaciones implementan un plan que no contempla los escenarios de errores en la recuperación de la información o simplemente no lo implementan.
- **Cuentas administrativas compartidas. -** El uso compartido de estas cuentas es un error de administración de los más graves, siendo así que pone a disposición de los usuarios pertenecientes al grupo la capacidad administrar otras cuentas de usuarios o grupos, de este modo se genera una vulnerabilidad de seguridad de alto nivel que compromete la administración de los servicios del Directorio Activo. (Ramirez Cuesta, 2014)

3.4. Configuración general del ambiente de pruebas

3.4.1. Características del ambiente de pruebas

Para generar el ambiente de pruebas virtualizado que emule un escenario de malas prácticas en Active Directory, es indispensable contar con las herramientas necesarias para su desarrollo, es así que en el presente trabajo se hace uso de las herramientas de hardware y Software necesarias que ayudan al análisis de la propuesta, de tal manera sus especificaciones son detalladas a continuación.

Características de Equipo para pruebas

Tabla 8. *Especificaciones de Equipo de pruebas*

Computadora para realizar el ambiente de pruebas	
Hardware	Descripción
Procesador	Intel(R) Core (TM) i5-7500 2.4GHz
Disco duro	1TB SSD
Memoria RAM	8GB 1600MHz

Tarjeta de Red	Realtek PCIe GbE Familia Controller
Sistema Operativo	Windows 10 Pro x64 bits

Fuente – Elaborado por el autor

Características de las máquinas virtuales

Tabla 9. *Especificaciones de máquina virtual servidor*

Características	**Domain Controller**	**Usuario del dominio**	**Kali Linux**
Procesador	Virtual de 2 núcleos	Virtual de 2 núcleos	Virtual de 2 núcleos
Disco duro	60 GB	60 GB	60 GB
Memoria RAM	2 GB	1GB	1GB
Tarjeta de Red	Realtek PCIe GbE Familia Controller – virtual	Realtek PCIe GbE Familia Controller – virtual	Realtek PCIe GbE Familia Controller – virtual

Características de Software

Tabla 10.*Requisitos de Software.*

Software necesario para generar el ambiente de pruebas	
Software	Versión
VMware Workstation	16 pro x64 bits
Windows 10	Pro x64 bits
Windows Server	2016 x64 bits
Kali Linux	2021.1

3.4.2. Configuración del ambiente de pruebas

Para la configuración del ambiente de pruebas se utiliza el software de virtualización VMware versión 16 Pro Workstation, mismo que permite crear máquinas virtuales, entre las cuales figura una para cada software. El desarrollo del ambiente de prueba requiere la creación de las maquinas virtual con las configuraciones de características que detallan la Tabla. 9 y software que se menciona en la Tabla 10, donde los pasos para configurar el ambiente son:

- Crear una nueva máquina virtual
- Elegir la imagen ISO del sistema operativo a implementar
- Definir la ruta de instalación
- Especificar el almacenamiento, memoria, procesadores, tipo de red, etc.

Este es un requisito previo para el desarrollo de cualquier ambiente de pruebas virtualizado, de modo que se convierte en la parte fundamental previa a la virtualización, así mismo se detallan los pasos de la configuración en el Anexo 1.2

3.4.3. Configuración de Active Directory con malas prácticas de seguridad

Como se había definido en los objetivos se hará la instalación configuración de los servicios de Active donde se evidencien el uso de malas prácticas, de tal forma que emule dicho escenario dando paso a la fase de análisis de vulnerabilidades.

Los servicios de Active Directory se instalan y configuran con ajustes predeterminados, durante el proceso se requiere el ajuste de los parámetros de red local, que se configuran de forma estática en la máquina del servidor local, como se muestra en la tabla 11.

Tabla 11. *Ajustes de red para Active Directory. Elaborado por el autor*

Red local	**DC-GYE**
IP	192.168.109.130
Mascara de red	255.255.255.0
Puerta de enlace	192.168.109.2
DNS	127.0.0.1

Fuente – Información tomada de investigación directa. . Elaborado por el autor

3.4.3.1. Instalación de roles y características

Una vez configurada la red se instalan los servicios de Active Directory con las configuraciones por defecto y sin tomar medidas de seguridad que emulen un escenario de malas prácticas en el proceso de instalación y configuración de estos servicios.

Figura 9. *Instalación de servicios de Active Director. . Elaborado por el autor*

Mala practica:

Se realiza la instalacion de un solo controlador de dominio, pese a que las recomendaciones del asistente recomienda tener un minimo de dos, con el fin de tener un respaldo de inicio de sesion en caso de fallos del servidor.

3.4.3.2. Configuración de la base de datos del directorio

En la configuración de las rutas de la base de datos, archivos de registro NTDS y la base de datos SYSVOL del directorio activo se configuran en las rutas predeterminadas de almacenamiento en el disco local C del mismo servidor.

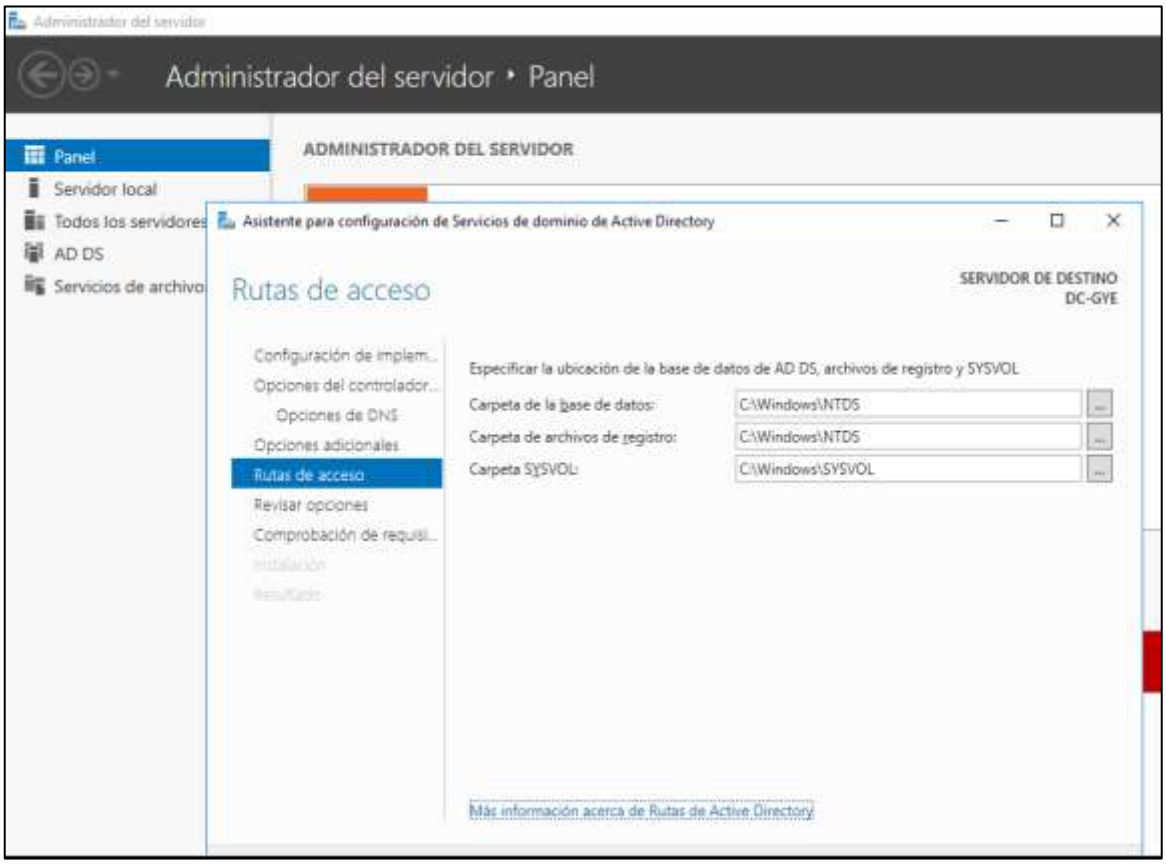


Figura 10. *Configuración de ruta de base datos de Active Directory. . Elaborado por el autor*

Mala práctica:

Definir rutas de almacenamiento de archivos de registro NTDS y la base de datos SYSVOL de forma predeterminada en el mismo Controlador de Domino en la partición C, compromete la disponibilidad de los recursos, ya que al tener un solo lugar de almacenamiento en caso de fallos de unidad la base de datos corre riesgo de perderse afectando los otros servicios, así mismo son un objetivo principal para atacantes que suelen buscar información en rutas predeterminadas.

3.4.3.3. Propiedades de Active Directory

Después del levantamiento de los servicios de Active Directory, se promueve el servidor Controlador de Dominio, creando un nuevo bosque con su dominio raíz "prueba. Local", donde este pertenece al servidor DC-GYE.

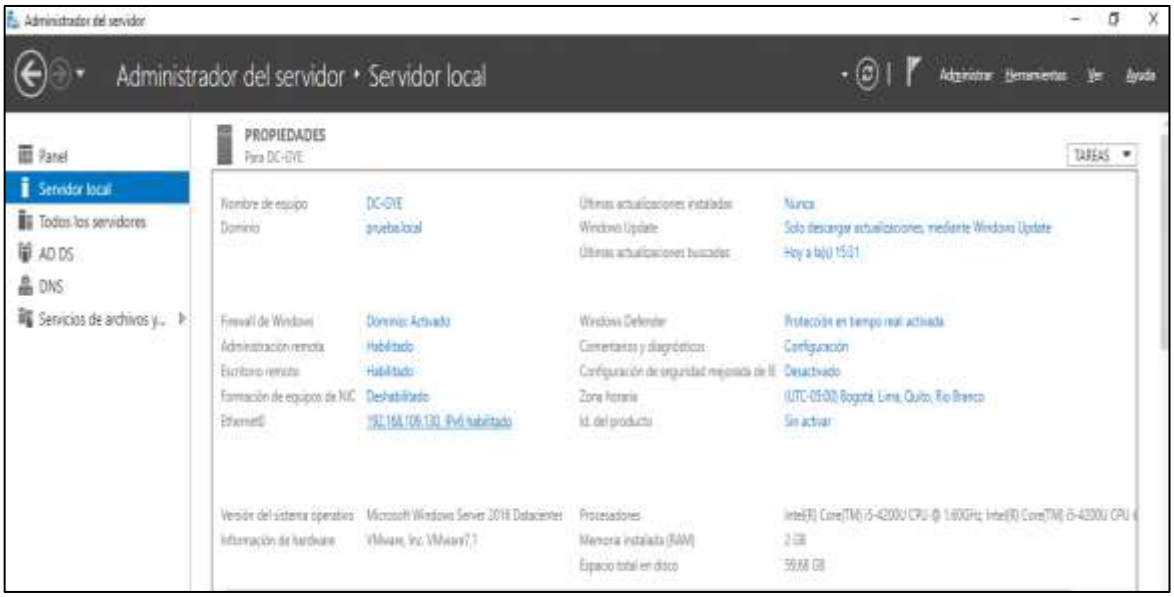


Figura 11. *Propiedades del servidor local. . Elaborado por el autor*

Mala práctica: La opción de escritorio remoto RDP se encuentra habilitada sin ninguna medida de protección adicional, así mismo la seguridad mejorada de IE (Internet Explorer) se encuentra desactivada, lo que puede ser perjudicial al comprometer directamente al directorio activo pudiendo ser objeto de ataques de malware o ransomware donde los ciberatacantes obtengan acceso privilegiado al sistema.

3.4.3.4. Creación de Unidades organizativas

Antes de agregar usuarios como parte de la estructura lógica de AD, se crean las Unidades Organizativas (OU) y subunidades OU, que sirven para segmentar las entidades de la organización y asignar políticas de grupo y delegación de privilegios administrativos.

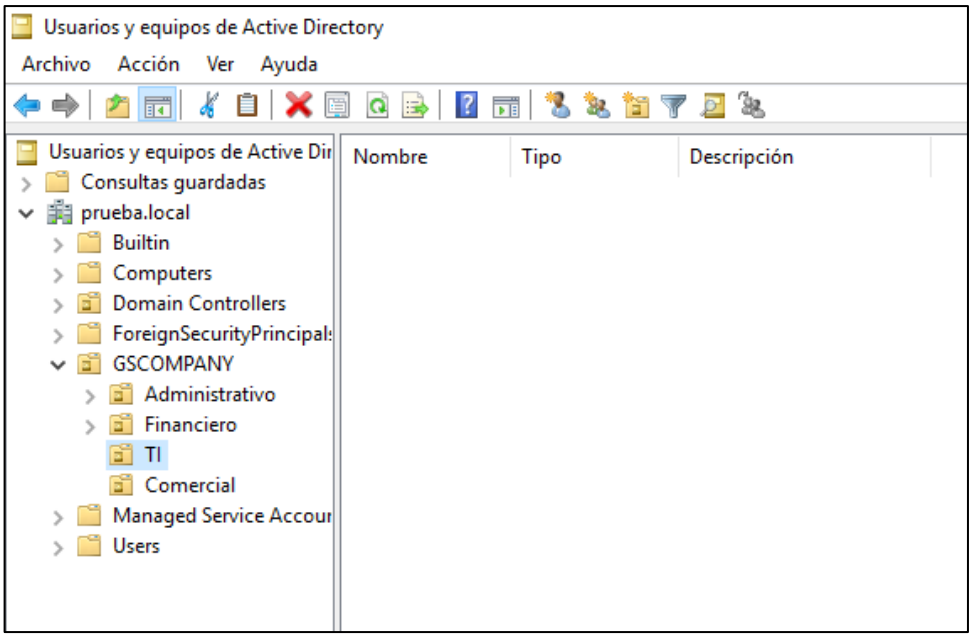


***Figura 12**. Unidades Organizativas (OU). Elaborado por el autor*

Mala práctica: Las OU se crean con nombres representativos de cada departamento, donde aparentemente se ve inofensivo, pero esto da paso a que los atacantes tengan objetivos de ataques más claros facilitándoles el trabajo de reconocimiento.

3.4.3.5. Creación de usuarios y equipos de trabajo

Después de crear las Unidades Organizativas, se crean los usuarios con nombre representativos de su cargo en la organización, asimismo la contraseña no puede ser cambiada y nunca espera, pero a su vez se utilizan contraseñas genéricas en todos los usuarios.

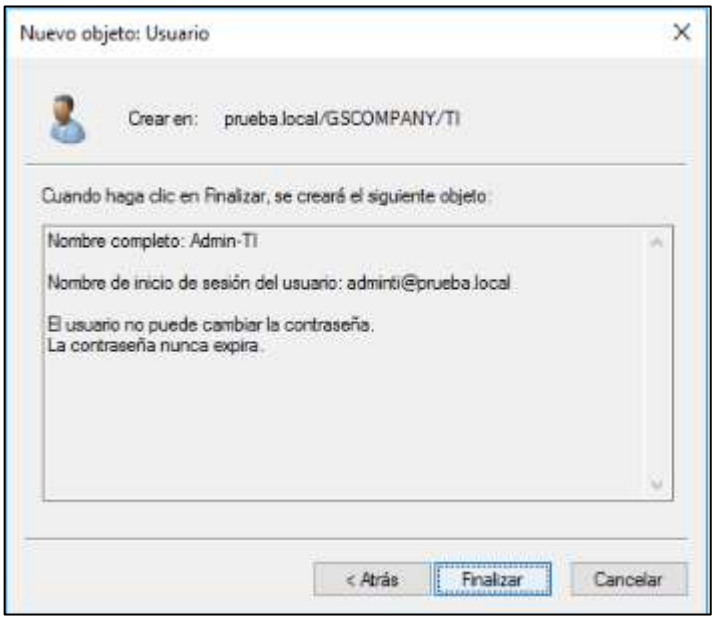


***Figura 13**. Creación de usuario del dominio Elaborado por el autor.*

Mala práctica: Crear usuarios con nombres representativos permite que los atacantes puedan identificar con mayor facilidad sus objetivos. Así mismo el uso de contraseñas genéricas que no caducan genera un alto riesgo de inseguridad ya que una vez comprometidas pueden ser usadas para que los atacantes mantengan el acceso dentro del directorio activo con las claves que han obtenido

3.4.3.6. Creación de grupos de seguridad

Se crean los grupos de seguridad pertenecientes al dominio, cuyos privilegios les permiten tener acceso a todos los recursos del directorio activo. En este caso se crea el grupo "Financiero" como grupo de seguridad dentro de la OU Financiero, para que los usuarios de este grupo accedan a los recursos compartidos de otros departamentos para definir los balances financieros de la empresa. De tal forma que el grupo y sus miembros pertenecen al grupo de administradores del dominio.

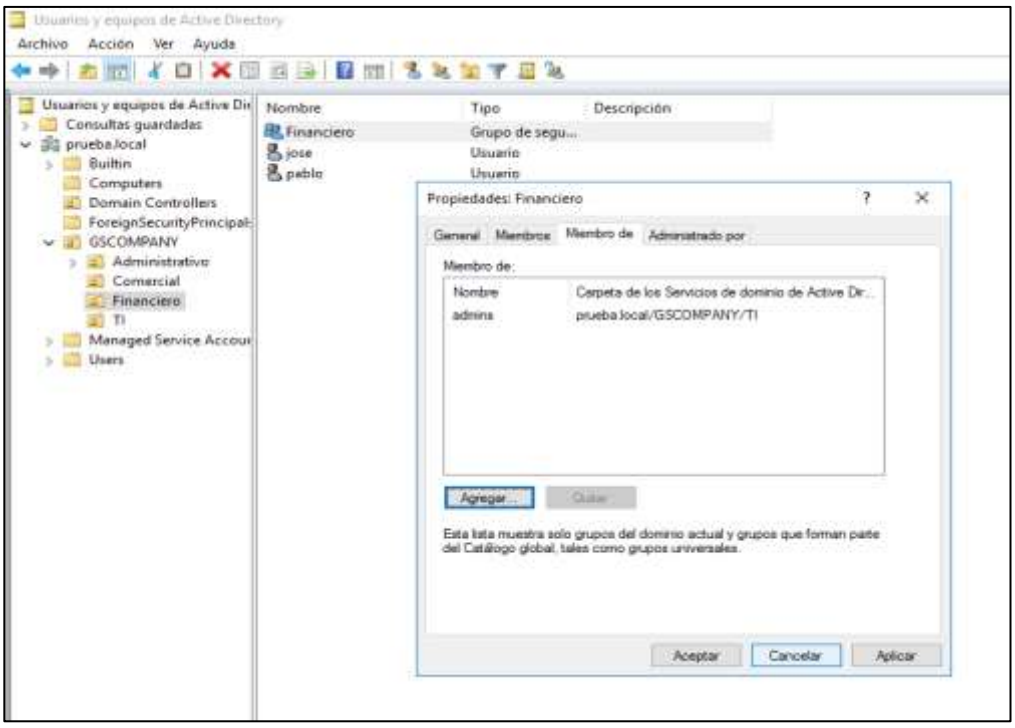


Figura 14.*Creación de Grupos de seguridad. Elaborado por el autor*

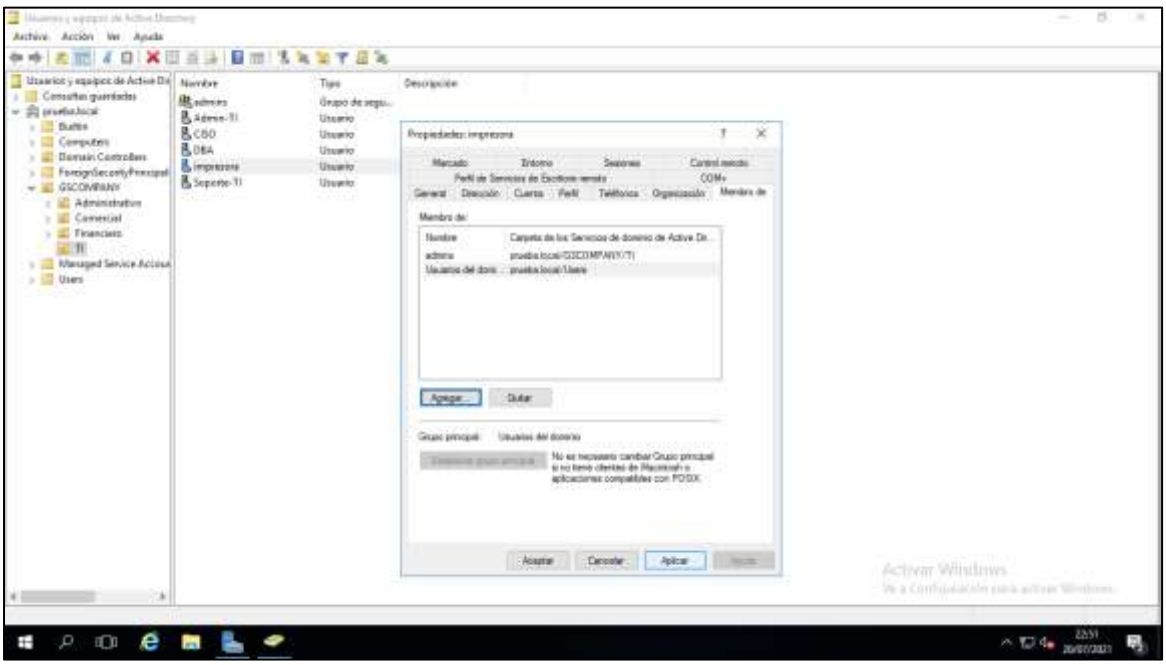
Mala práctica: Hacer que un grupo de seguridad y sus miembros pertenezcan al grupo de administradores del dominio, les brinda total libertad sobre los recursos y configuraciones el directorio activo, por lo que las consecuencias de esta mala práctica brindan la posibilidad los atacantes hacerse miembros del grupo con un robo de credenciales y obtener el acceso

privilegiado. Por lo que para crear un grupo de seguridad debe verificar y restringir solo los recursos que necesite acceder.

3.4.3.7. Cuentas de servicios

Se crean las cuentas de servicios para que se ejecuten en el sistema operativo de Windows Server, en este caso la cuenta impresora es creada en la OU TI ya que son los encargados de los equipos informativos del director, esta cuenta sirve para ejecutar los servicios de impresión en más de un equipo misma que perene al grupo de Administradores del dominio.

Figura 15. *Cuenta de servicios. Elaborado por el autor*



Mala práctica:

La creación de cuentas de servicios genéricas que no tengan caducidad de contraseñas y pertenezcan a un grupo administrativo es un riesgo de seguridad, si estas son comprometidas en un ataque de escalado de privilegios por lo que es necesario aplicar restricciones necesarias a estas cuentas dentro de su configuración.

3.4.3.8. Configuraciones de GPO

Las políticas de grupo que controlan el entorno de cuentas de grupos y usuarios del directorio activo se establecen por defecto para todos los grupos del dominio con la instalación de los servicios de Active Directory, que incluyen las directivas de contraseñas y de inicio de sesión con Kerberos.

Figura 16. Configuraciones de GPO. Elaborado por el autor.

Mala práctica:

No se realiza la configuración de GPO para las diferentes unidades organizativas y los equipos de estas aparte de las que se establecen por defecto, asimismo no se ajustan políticas de auditoria no permiten realizar una trazabilidad a los eventos en el Controlador de Dominio.

3.5. Pruebas de pentesting para el análisis de vulnerabilidades.

Una vez concluida la fase de instalación y configuración de los servicios de Active Directory en la máquina virtual servidor, se desarrolla uno de los objetivos principales de este trabajo de investigación. Es así que con tal de identificar las vulnerabilidades de seguridad que generan las malas prácticas ejecutadas anteriormente se realiza el proceso de pruebas de pentesting utilizando herramientas para la identificación de vulnerabilidades. De modo que la investigación requiere analizar e identificar vulnerabilidades no se requiere verificar la explotación de estas, por lo tanto, se utilizan las tres primeras fases del pentesting:

- Reconocimiento
- Escaneo
- Enumeración

En igual forma durante el proceso de cada fase de pentesting se determina el impacto que dichas vulnerabilidades generan a nivel de seguridad de la información.

3.5.1. Fase de reconocimiento

Reconocimiento con Rsop.msc

Desde el equipo cliente que se encuentre unido al dominio, se ejecuta el comando de informe Rsop.msc, cuyas siglas significan (Resultan Set o Policy), cuya función extrae un informe detallado de todas las configuraciones de las GPO aplicadas en usuarios y equipos del Active Directory de manera detallada. La sintaxis de este comando es **rsop.msc**.

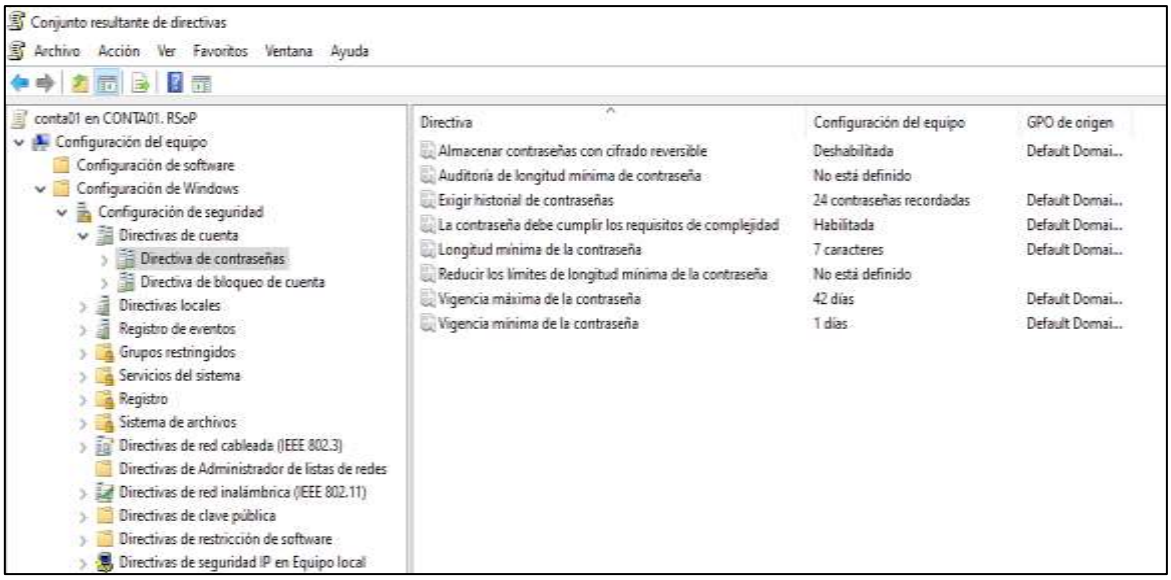


Figura 17. *Resultado de informe Rsop.msc Elaborado por el autor.*

Una vez ejecutado el comando desde el comando ejecutar (Ctrl+R), se obtiene la información de las GPO aplicadas a grupos usuarios, lo que permite verificar el nivel de seguridad a nivel de políticas en Active Directory.

Tabla 12. *Vulnerabilidades identificadas con Rsop.msc*

Vulnerabilidades	Impacto
• **Las políticas de grupo aplicadas al usuario están por defecto** • **El acceso a la ejecución de comandos de administrador con cmd.**	Las políticas por defecto permiten que los miembros y grupos del directorio activo no tengan restricciones, dándoles paso libre que brinda la posibilidad de en caso de robo de credenciales los malos actores tendrán libre acceso a varias funciones del equipo que se encuentre en el dominio.

Fuente – Información tomada de investigación directa. . Elaborado por el autor

Reconocimiento con GPRESULT/ R

Se muestran los resultados de la ejecución de este comando desde un ordenador perteneciente al dominio, donde se muestra en pantalla la configuración de las directivas de grupo aplicada en el equipo, la versión del sistema operativo, el perfil de usuario, el nombre del sitio y el tipo de enlace, del dominio de manera más específica.

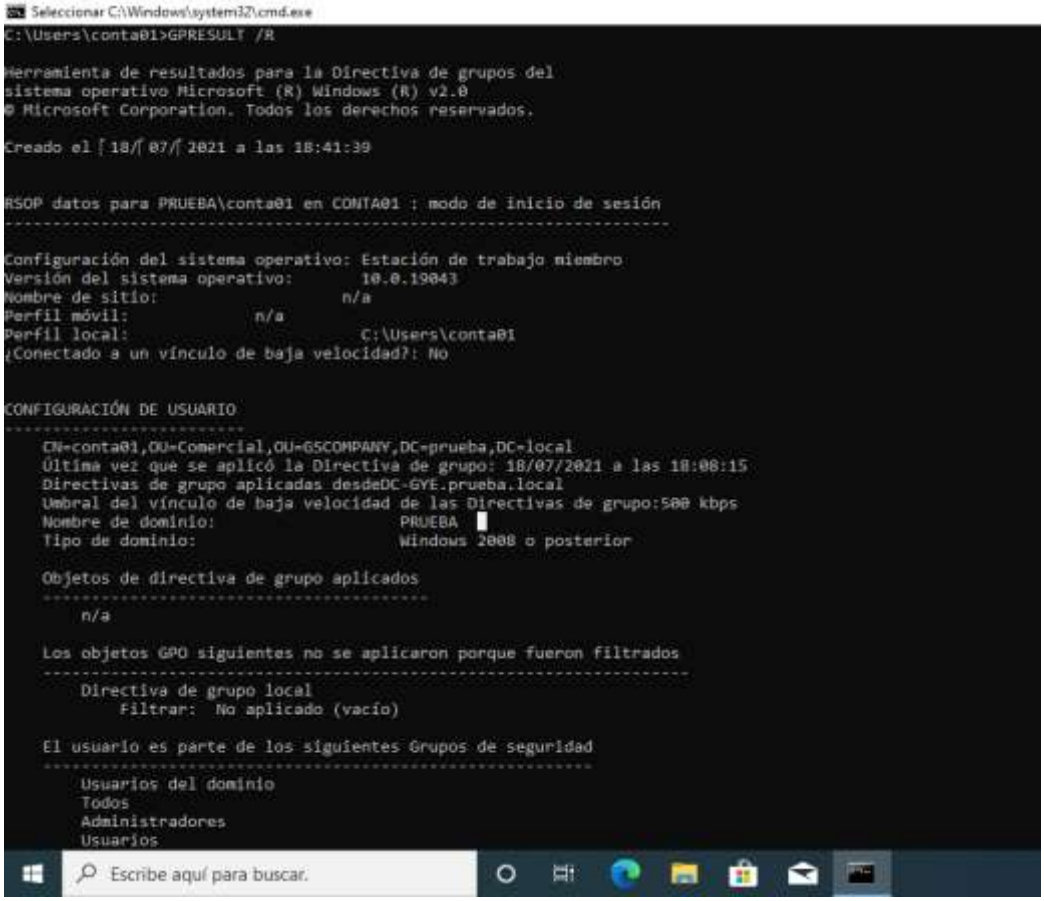


Figura 18. *Resultados de GPRESULT. Elaborado por el autor*

Tabla 13. *Reconocimiento con GPRESULT /R. Elaborado por el autor*

Vulnerabilidades	Impacto
• **Las políticas de grupo y datos de inicio de sesión están expuestas.** • **Toda la configuración de las GPO del usuario.**	El reconocimiento de esta información da paso a que se materialicen ataques focalizados, de modo que al obtener esta información definan al objetivo de manera más ágil.

Fuente tomada de investigación directa. Elaborada por el autor

Reconocimiento con Net User

La ejecucion de este comando brinda informacion de el usuario y demas cuentas que se encuentran dentro del dominio, como inicio de sesion y actividades de la cuenta, de la misma forma si se aplica el comando net user/ domain " nombre de usuario", se obtiene informacion detallada de el usuario seleccionado.

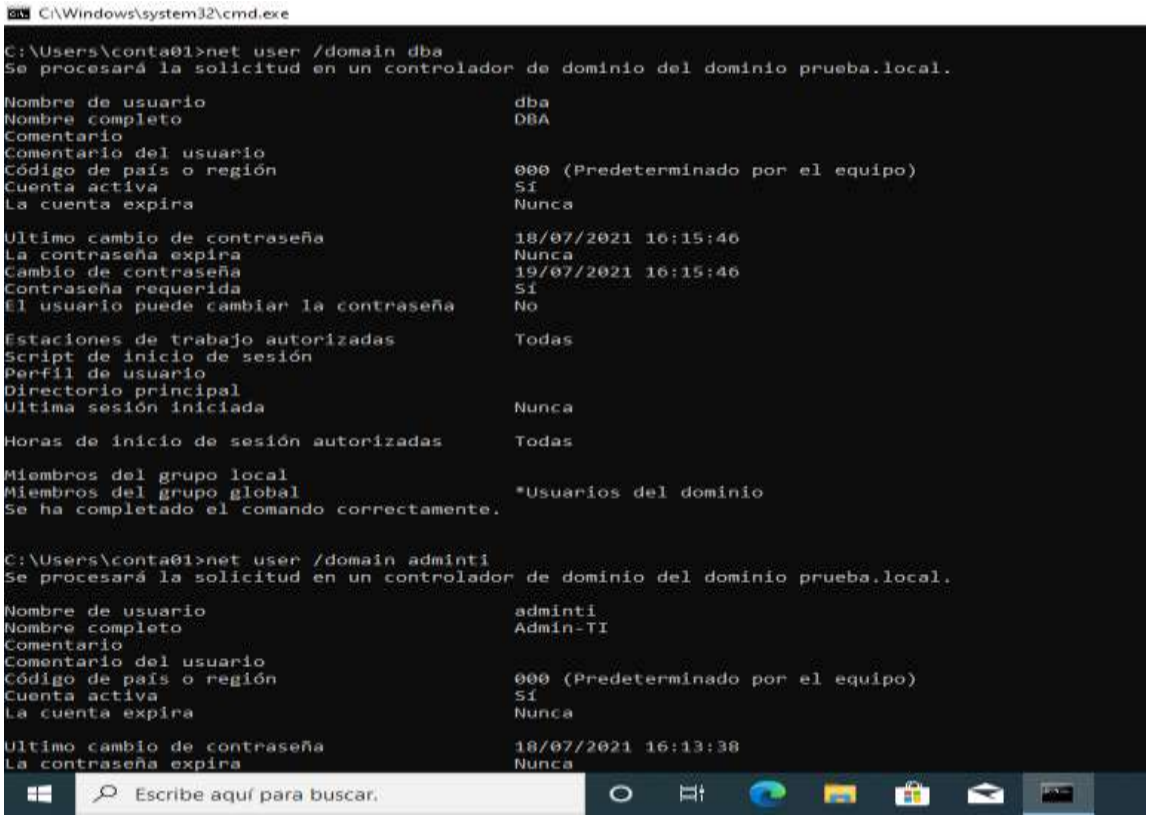


***Figura 19**. Reconocimiento con Net user Elaborado por el autor.*

***Tabla 14.** Vulnerabilidades con Net user. Elaborado por el autor*

Vulnerabilidades	Impacto
• **Contraseñas sin caducidad** • **Nombres identificables** • **Cuenta sin caducidad** • **Registros de inicios de sesión**	Tener una contraseña sin caducidad permite que un ataque de escala de privilegios se pueda materializar con exploits *backdoors* y mantener un acceso, además de que con los registros de inicio de sesión se puede encontrar cuentas inactivas, lo que representa un objetivo para el acceso privilegiado.

Fuente tomada de investigación directa. Elaborada por el autor

3.5.2. Fase de escaneo

Escaneo con Nmap

Esta herramienta es ejecutada en la maquina Kali Linux, la misma que incluye varios comandos para el escaneo de puertos y servicios que se encuentran activos en el sistema operativo de la maquina a auditar. Una vez inicializado se ejecuta para el escaneo de puertos e identificación de los servicios, sistema operativo y versiones de los servicios que se están ejecutando, donde su sintaxis es: **nmap -O -sV 192.168.109.130**

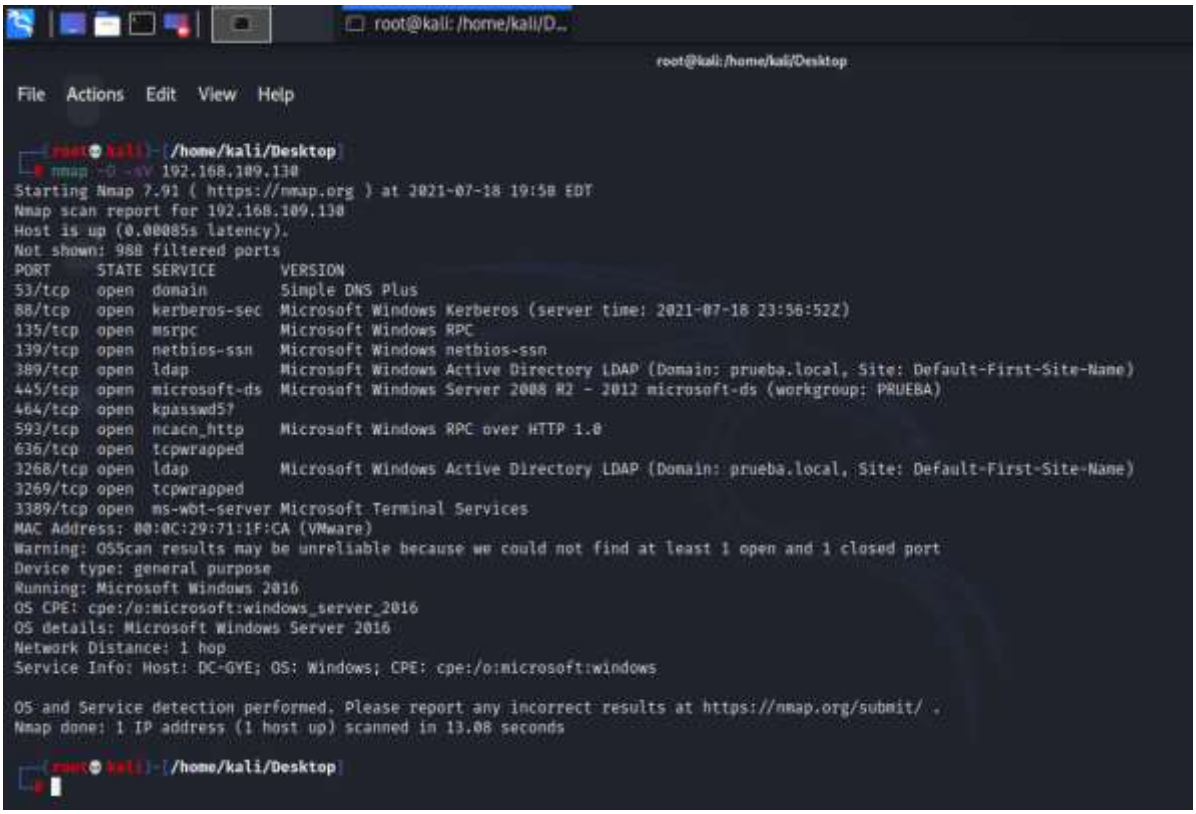


Figura 20. *Escaneo de puertos con Nmap. Elaborado por el autor*

Tabla 15. *Vulnerabilidades en puertos con Nmap.*

Vulnerabilidades	Impacto
• **Múltiples puertos TCP de servicios importantes abiertos como el 88, 389, 135 y el 139.**	Los puertos abiertos representan un peligro para diferentes amenazas desde acceso no autorizado, ataques de fuerza bruta hasta la aplicación de ataques DoS.

Fuente tomada de investigación directa. Elaborada por el autor

De igual forma se aplica el escaneo de vulnerabilidades con el script integrado vulscan.nse, este realiza la búsqueda de servicios contra sus scripts y determina las vulnerabilidades que se cotejan con bases de datos de vulnerabilidades, donde su sintaxis de ejecución es **nmap --script vuln.**

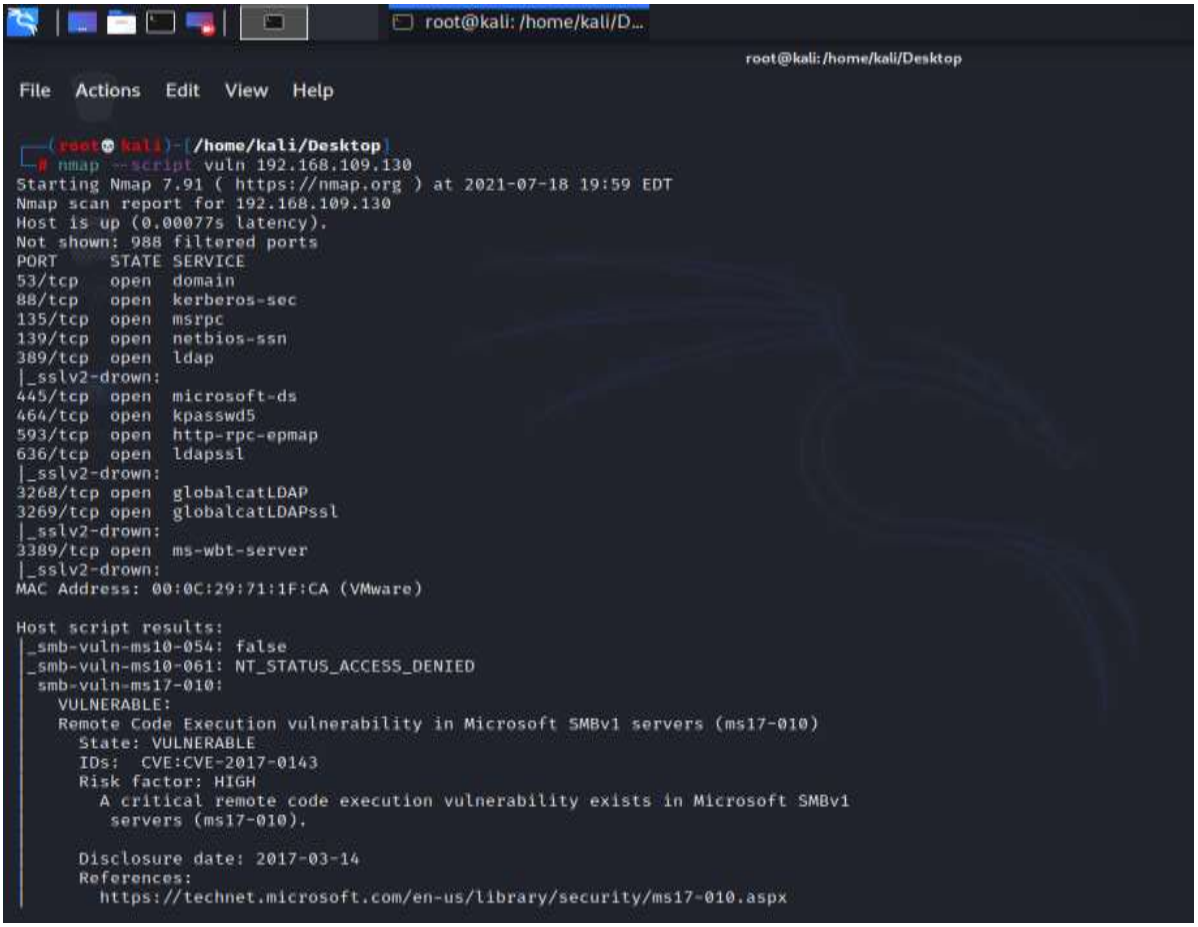


Figura 21. *Escaneo con buscan en Nmap. Elaborado por el autor*

Tabla 16. *Vulnerabilidades con vulscan Nmap.*

Vulnerabilidades	Impacto
• **VulnerabilidadCVE-2017-0143 asociada al puerto 135 TCP para el servicio RPC para la ejecución remota de código en Microsoft SMBv1 servidores**	Esta vulnerabilidad representa un riesgo para ataques de tipo ransomware, de tal forma que permite a los atacantes ejecutar código malicioso atravesó de paquetes diseñados, lo que compromete la integridad, disponibilidad y confidencialidad del sistema.

Fuente tomada de investigación directa. Elaborada por el autor

Escaneo con Nessus

Una vez que se evidenciaron vulnerabilidades en los puertos y servicios con Nmap, se aplica un escaneo más profundo con Nessus 8.15.0, sobre Kali Linux, cuya ventaja es el escaneo y clasificación del riesgo de las vulnerabilidades basado en el Sistema Común para la Puntuación de vulnerabilidades 3.0 (CVSS), cuya métrica de medición es:

CVSS	SEVERIDAD	DESCRIPCION
9.0 - 10	Critico	Servicios desactualizados, vulnerabilidades de denegación de servicios, ejecución de código arbitrario.
7.0 - 8.9	Alto	Fuga de información sensible, inyección en intercepción de datos, servicios públicos no permitidos.
4.0 - 6.9	Medio	Certificados SSL no confiables, generadores aleatorios predecibles, fuga de información, navegación de directorios.
0.1 - 3.9	Bajo	Protocolos de comunicación no segura, servidores no encriptados, creación de archivos temporales no seguros.
0.0	Ninguno	No existe ningún factor de riesgo.

Figura 22. *Métrica de vulnerabilidades CVSS. Tomado de Anexo B de Verificación del grado de inseguridad de las infraestructuras de directorio activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado (2020).*

Después de elegir como objetivo la dirección del servidor se realiza el escaneo que arroja los resultados que incluyen la cantidad de vulnerabilidades identificadas de forma clasificada.

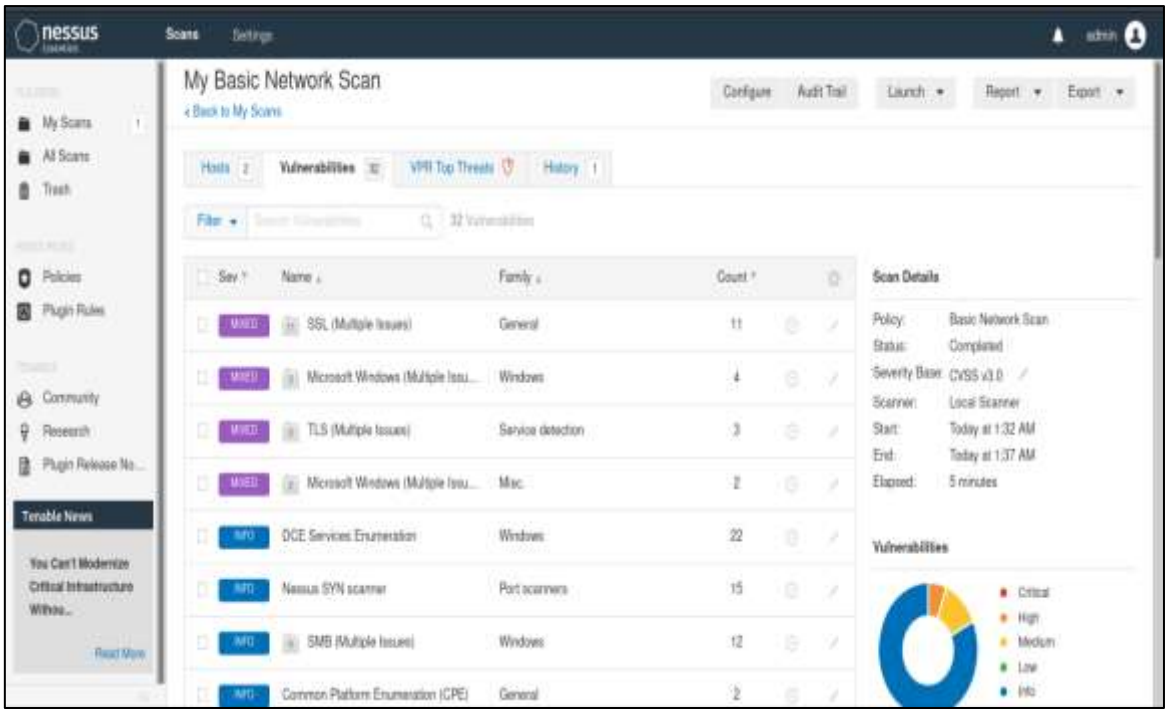


Figura 23. *Resultados de escaneo de vulnerabilidades con Nessus. Elaborado por el autor*

Asimismo, una vez concluido el análisis los resultados son exportados en un archivo PDF, cuyo contenido incluye las diferentes vulnerabilidades identificadas clasificadas con la métrica presentada en la **Figura 21**.

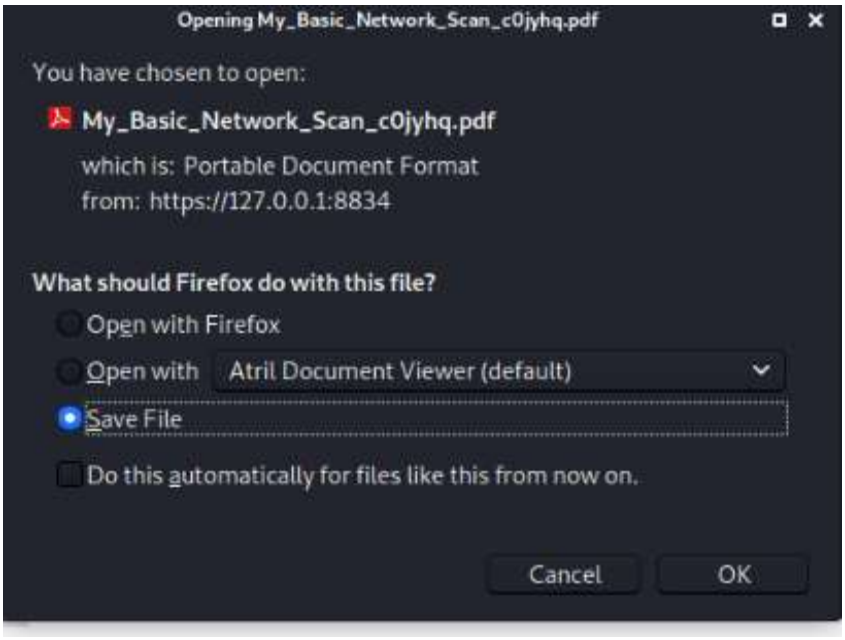
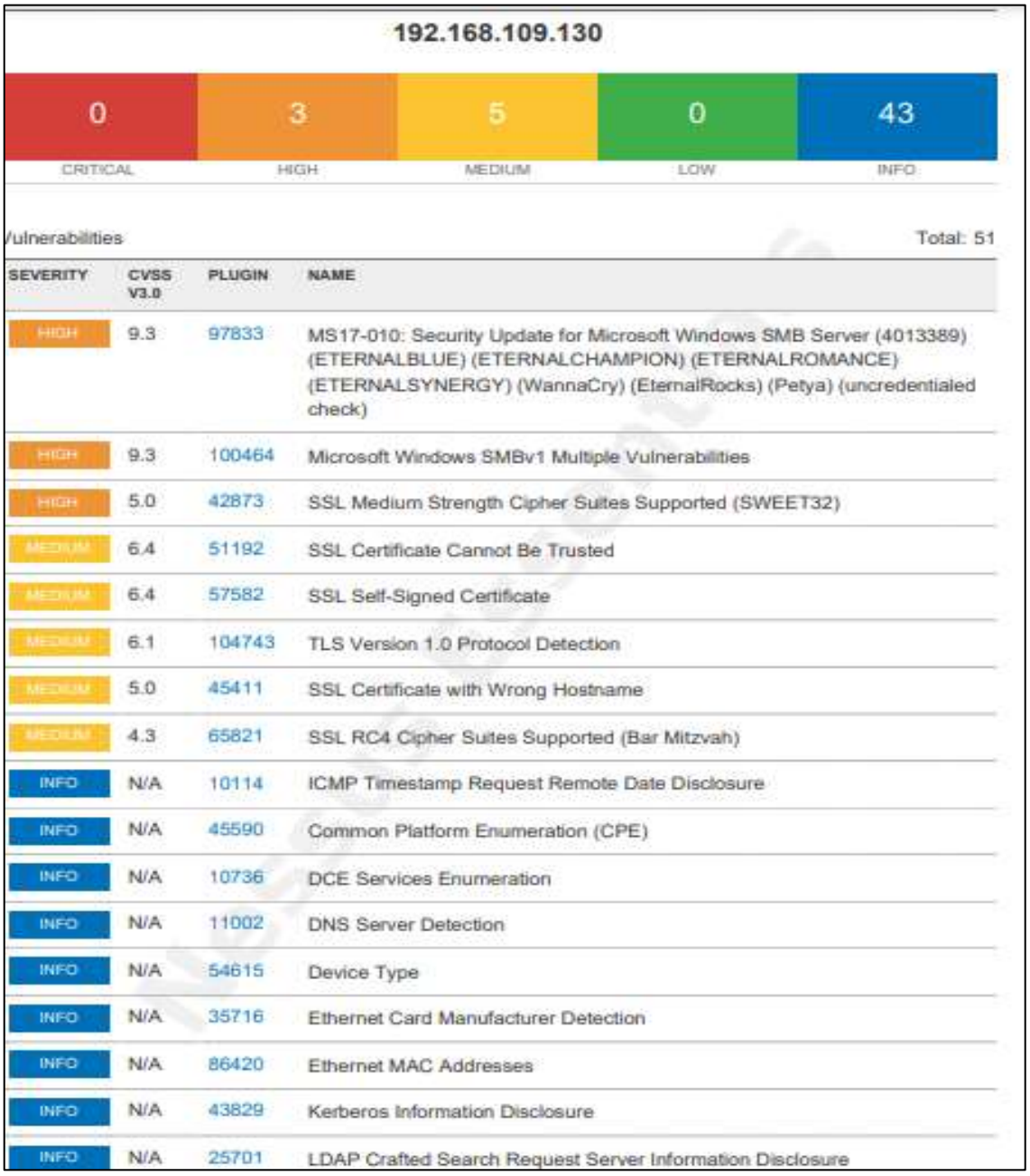


Figura 24. *Exportación del informe de análisis de vulnerabilidad con Nessus. Elaborado por el autor*

El informe revela un total de 51 vulnerabilidades escaneadas, de las cuales 43 no representan un riesgo inminente, 0 de bajo riesgo, 5 de riesgo medio, 3 de alto riesgo y 0 de riesgo crítico. Asimismo, su calificación de riesgo y el nombre que la identifica.



192.168.109.130

0	3	5	0	43
CRITICAL	HIGH	MEDIUM	LOW	INFO

/ulnerabilities — Total: 51

SEVERITY	CVSS V3.0	PLUGIN	NAME
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	9.3	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure

Figura 25. *Resumen de vulnerabilidades identificadas con Nessus. Tomado de Informe de principales vulnerabilidades. . Elaborado por el autor*

Pero lo que más destaca de este informe es su identificación de complemento (Plugin), cuyo código direcciona a la página de Tenable, donde se encuentra mayor información de la vulnerabilidad y la solución que se de aplicar para mitigarla, como se muestra en la siguiente tabla resumen de la información encontrada.

Tabla 17. Resumen de vulnerabilidad MS17-01

Gravedad	Nivel CVSS V3.0	ID	Nombre	Descripción	Solución
Alta	9.3	97833	MS17-010: Actualización de seguridad para Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (verificación sin credencial)	• Existe una vulnerabilidad de divulgación de información en Microsoft Server Mensaje Block 1.0 (SMBv1) debido a un manejo inadecuado de determinadas solicitudes. Un atacante remoto no autenticado puede aprovechar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. • ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y exploits de Equation Group divulgados el 14 de abril de 2017 por un grupo conocido como Shadow Brokers. WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades de Equation Group	Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también ha lanzado parches de emergencia para los sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8.

Información tomada de investigación directa. Elaborada por el autor

3.5.3. Fase de enumeración

Enumeración con NTBSCAN

Con la ejecución de esta herramienta se enumera la información de un rango de direcciones para la identificación de los nombres NETBIOS abiertos en una red TCP / IP local o remota. De tal forma que se extra la información del nombre de NetBIOS del rango de direcciones 192.168.109 /24 e identifica cuales pertenecen al servidor y su dirección MAC.

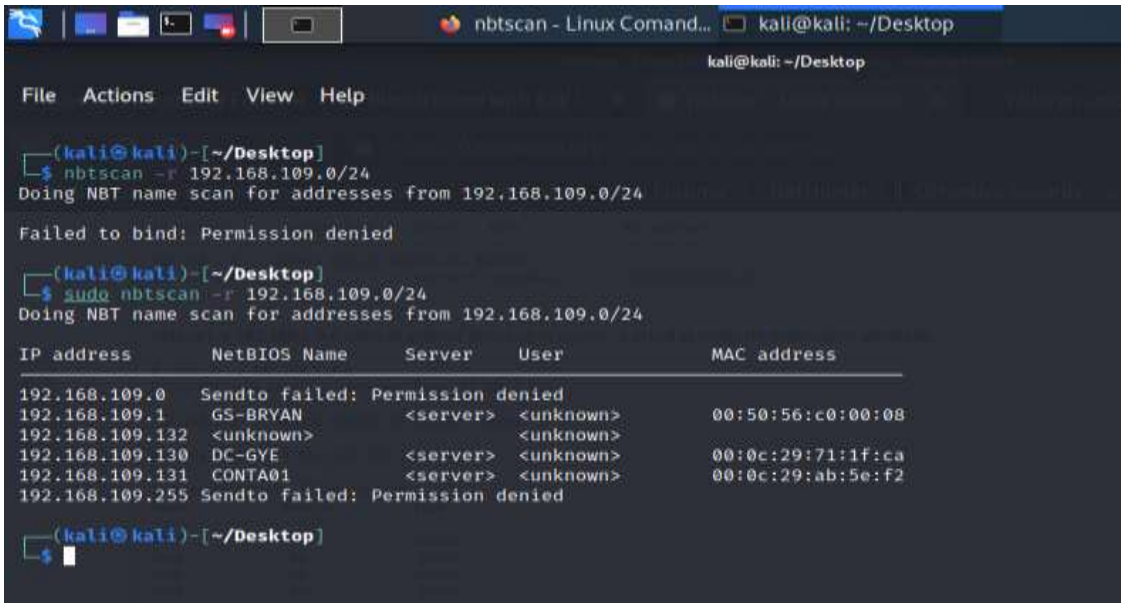


Figura 26. *Enumeración de direcciones con NTBSCAN. Elaborado por el autor*

Enumeración con Enum4linux

Los resultados de enumeración con esta herramienta permiten identificar la información del objetivo, obteniendo el rango de RID, el nombre del grupo de trabajo que es PRUEBA. De tal forma que esta información se utiliza para la identificación y selección de los objetivos.

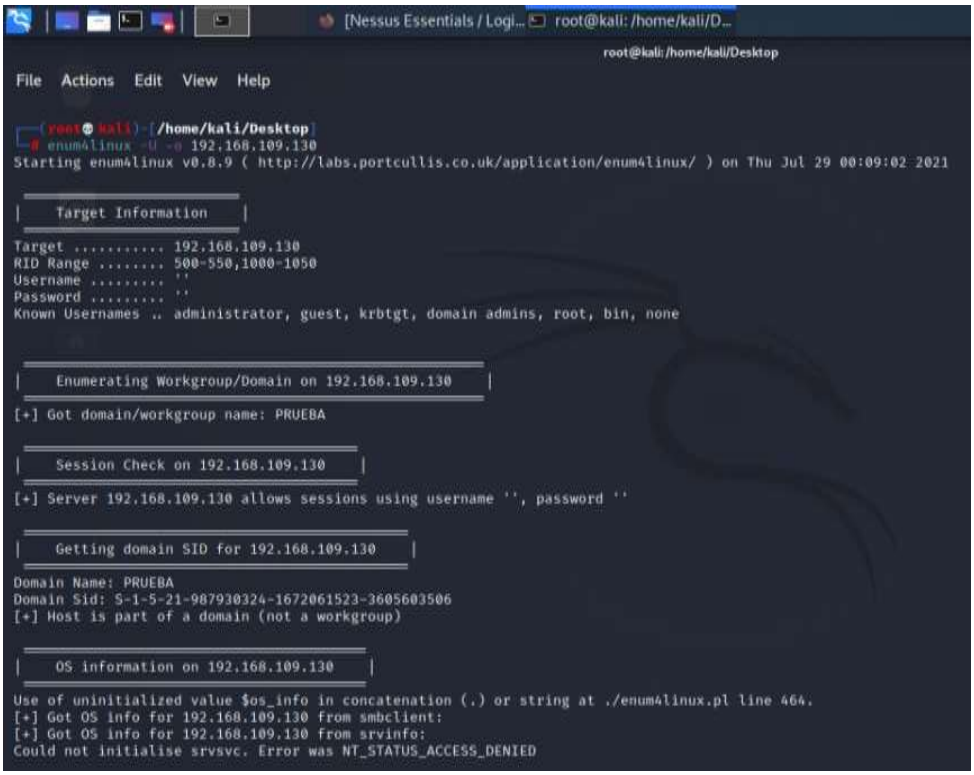


Figura 27. *Enumeración con Enum4linux. Elaborado por el autor*

3.6. Lineamientos para definir Políticas de seguridad de la información

Una vez identificadas las vulnerabilidades y el impacto potencial de las mismas durante la etapa de pruebas de pentesting, se determina que representan un riesgo de seguridad para los servicios de Active Directory, por lo que es necesario definir políticas que se ajusten al objetivo de reducir los niveles de riesgo en la organización. Sim embargo no se pueden para definir políticas de seguridad de la información de forma específica debido a que estas deben ser establecidas en base a los objetivos y requerimientos de la organización, en concordancia con la guía de implantación de políticas de seguridad de la información en la norma UNE-EN ISO/IEC 27002:2017.

Por lo tanto con base en las normativas internacionales de seguridad de la información, se definen los lineamientos necesarios que deben incluir el desarrollo de las políticas de seguridad para asegurar una correcta implementación y administración de los servicios de Active Directory. En el mismo sentido se identificar los aspectos que más significativos en el marco de seguridad de la información como lo son

- Gestión de accesos
- Gestión de privilegios
- Gestión de protección

- Gestión de incidentes

Tomando en consideración lo expuesto anteriormente es comparado con las normativas y controles de seguridad de la información que cubran tales aspectos al momento de definir políticas de seguridad.

3.6.1. Gestión de acceso.

El control de acceso a la información es uno de los aspectos fundamentales para al momento de definir una política, a causa de que es el primer objetivo que establecen los atacantes para comprometer la seguridad de la información. Así mismo el usuario debe tener acceso a la información, sin embargo, el acceso a la información debe estar acorde al rol y responsabilidad que desempeña dentro de la organización.

Tabla 18. *Lineamientos para políticas de Gestión de acceso.*

Lineamiento	Descripción	Normativa referente
Acceso lógico	A modo de proporcionar el idóneo acceso a la información, es necesario que las políticas de control de acceso deben garantizar el acceso a los recursos específicos del sistema y el tipo de acceso permitido de maneras segura, de tal forma se aplique a: • Cuentas de usuario • Separación de tareas • Acceso a recursos de información • Acceso privilegiado • Accesos remotos	• NIST SP 800-12 – control: 10.1
Autenticación y contraseñas	Con el fin de garantizar un control de acceso seguro al sistema de forma lógica, es necesario las políticas a desarrollar tomen en cuenta los aspectos de seguridad que ayuden a mantener la confidencialidad de la información tales como: • Acuerdo de confidencialidad • Verificación de identidad • Credenciales individuales • Contraseñas seguras y robustas • Periodo de caducidad y cambio de contraseñas	• UNE-EN ISO/IEC 27002:2017 - Control 9.2.3 Gestión de privilegios de acceso
Acceso a la red y comunicaciones	Con respecto al acceso de la seguridad de las redes, las políticas deberán estar alineadas a controles y monitoreo de actividades de las comunicaciones dentro de los limites externos y los	• UNE-EN ISO/IEC 27001:2017- control: A.13.1

	limites internos dentro del sistema, así como también garanticen que la infraestructura de TI y configuraciones de red se alineen a controles de seguridad que reduzcan niveles de riesgo que contemplen e: • Deshabilitar puertos inactivos • Segmentación de redes • Monitoreo de conexiones de red • Seguridad perimetral • Cifrado de conexiones remotas	• NIST SP 800-12-control 10.19

Fuente – Información tomada de investigación directa. Elaborado por el autor

3.6.2. Gestión de Privilegios

Los privilegios que se asignan dentro del sistema de Active Directory tiene un papel importante al momento de asignar restricciones de seguridad que sirven para marcar los límites de acceso a la información que el usuario puede llegar obtener, de modo que la asignación de estos deberá ser acorde a los roles y responsabilidad que se desempeñen en la organización debido a que dependiendo del nivel de estos sus acciones afectan de manera positiva o negativa a la continuidad de las actividades de la organización.

Tabla 19*. Lineamientos para la gestión de privilegios. Elaborado por el autor*

Lineamiento	Descripción	Normativa referente
Privilegios de grupos y usuarios	Las políticas que se generen deben designar los derechos para cada tipo de usuarios y sean asociados de acuerdo a las competencias dentro de la organización ayudando ´teniendo en cuenta que se deben aplicar medidas para: • Instalación y acceso a programas • Restricción de acceso a la información • Control sobre utilidades de sistema • Derechos de usuarios • Registro de asignación de privilegios •	• UNE-EN ISO/IEC 27002:2017 – controles: 9.4.4 y 9.2.5
Roles y responsabilidades	Debe existir una previa asignación de roles y responsabilidades dentro de la organización que permita determinar responsabilidades y tareas relacionadas a la seguridad de la información, por lo tanto, las políticas emitidas deben considerar incluir • Documentación de roles y responsabilidades • Designación de roles administrativos y estándares • Monitoreo del cumplimiento de roles y responsabilidades	• NIST SP 800-12 R-Capitulo 3 • UNE-EN ISO/IEC 27002:2017- Control: A.6.1.1

Fuente – Información tomada de investigación directa. Elaborado por el autor

3.6.3. Gestión de prevención

Como parte de las medidas de seguridad dela información, es preciso acordar parámetros que se alinean a la políticas contra incidentes de seguridad, donde se apliquen controles y medidas que estén dentro del marco de la prevención de eventos que comprometan la disponibilidad, integridad y confidencialidad de la información. De modo que con el fin de prevenir el progreso de vulnerabilidades en Active Directory sus políticas deben alinearse a los siguientes lineamientos.

Tabla 20. *Lineamientos para la gestión de prevención. Elaborado por el autor*

Lineamiento	Descripción	Normativa referente
Medidas de protección	Este lineamiento hace referencia a que las políticas adopten medidas de seguridad adecuadas para la protección donde se contemple: • Protección contra amanezcas internas y externas del sistema • Copias de seguridad • Integridad y confidencialidad de la información • Monitoreo de redes internas • Protección contra código malicioso • Cifrado de datos	• UNE-EN ISO/IEC 27001:2017 – controles: A.13.1.1, A.12.3, A.12.2.1 • NIST SP 800-12 R-10.20, 9.1.1
Monitoreo y auditoria	Con el fin de verificar que se cumplan los objetivos de seguridad de la información, las políticas de seguridad deben incluir aspectos relacionados a la comprobación de cumplimiento de parámetros de seguridad, por lo que su desarrollo debe incluir: • Registros de eventos • Monitoreo y revisión de las operaciones del sistema • Supervisión del cumplimiento de normas de seguridad • Revisión periódica programa • Uso del plan de seguridad	• UNE-EN ISO/IEC 27002:2017 controles: 18.2.2 • NIST SP 800-12 R-7.3.2.2, 7.3.2.3

Fuente – Información tomada de investigación directa. Elaborado por el autor

3.6.4. Gestión de incidentes

Debido a que los sistemas están expuestos a una serie de amenazas que pueden afectar la continuidad de las actividades de la organización, que van desde archivos maliciosos hasta desastres ambientales, por lo que aplicar métodos y controles como plan de contingencia

en caso de incidentes de seguridad dan paso a que se genere una respuesta en caso de un evento que afecte a la continuidad de la operaciones del sistema, pues en efecto se determina que las políticas de seguridad de la información se ajusten con lineamientos que garanticen una preparación en contra de incidentes de seguridad.

Tabla 21. *Lineamientos para la gestión de incidentes. Elaborado por el autor*

Lineamiento	Descripción	Normativa referente
Equipo de respuesta	Establecer una políticas de seguridad que incluya la asignación de un equipo respuesta contra incidente, de tal forma que se asignen roles y responsabilidades para mitigar amenazas de seguridad que atenten contra la continuidad de negocio, es decir deberán incluir: • Designación de responsabilidades • Monitores notificación de incidentes • Capacitación de respuesta	• 29 UNE-EN ISO/IEC 27001:2017 Controles :A.16.1 • COBIT 5- A.3
Manejo de incidentes	Para el manejo de incidentes de seguridad deben existir políticas que cubra los procedimiento a seguir dentro plan de contingencia de seguridad de la información como son: • Evaluar y decidir sobre el evento • Recopilación de información del evento • Contención de la amenaza y asilarla	• UNE-EN ISO/IEC 27001:2017 controles: A.16 • NIST SP 800-12 R – 10.9

Fuente – Información tomada de investigación directa. Elaborado por el autor

3.7. Conclusiones y Recomendaciones

3.7.1. Conclusiones

- Los resultados de la investigación documental y entrevistas, se concluye que existe un nivel considerable de vulnerabilidades en los servicios de Active Directory que se encuentran expuesta a diferentes amenazas externas e internas de seguridad informática que pueden son aprovechadas por atacantes para toma d acceso privilegiado.
- En la actualidad el servicio de Active Directory es la herramienta de gestión de archivos y usuarios usada por alrededor del 90% de empresas, por lo tanto, es objetivo principal en más del 80% de los ataques efectuados para obtener los accesos privilegiados dentro de las empresas, en concordancia con lo expuesto por (Felix Xavier & Javier Ernesto, 2018) donde concluyen que el los servicios de Active Directory tiene muchos mas vulnerabiliades que otros por lo tanto estan mas expuestos a las amenazas de seguridad de la informacion.
- La emulación del entorno de red centralizada basada en el uso de los servicios de Active Directory en Windows Server 2016 permite recrear escenarios de malas prácticas de seguridad en las etapas de instalación y configuración, logrando identificar las vulnerabilidades que se generan por dichas malas prácticas. Por consiguiente, se determina que el factor humano inlfuye de manera decisiva al momento de asegurar los serviicxios de Active Directory debido a que este actua de administrador de configuraciones de seguridad y usuario final del sistema.
- Durante la fase de pruebas de pentesting en conjunto sus herramientas se logran identificar las vulnerabilidades que se generan por malas prácticas de seguridad mismas que exponen a los sistemas d información a las amenazas existentes en ausencia de una previa consolidación de políticas de seguridad de la información que sirva como guía de controles para garantizar la confidencialidad, integridad y disponibilidad de la información y reducción de riesgos.
- La definición de lineamientos para la emisión de políticas de seguridad de la información dentro un marco metodológico de seguridad permite que los administradores de red puedan establecer planes de acción como contingencia para

la minimizar riesgos d seguridad como parte de las medidas para el aseguramiento de los servicios de Active Directory y cualquier otro sistema de información.

3.7.2. Recomendaciones

- Para el desarrollo y pruebas de pentesting que ayuden a identificar vulnerabilidades y riesgos potenciales, se recomienda utilizar las técnicas de virtualización de sistemas dado que estas se encuentran en ambientes controlados, lo que permite emular diferentes escenarios con riesgos de seguridad.
- Se recomienda un análisis periódico de los servicios de Active Directory, con la finalidad de identificar fallos de seguridad que permitan fortalecer la seguridad de los servicios de Active Directory.
- Antes de la implementación es recomendable que definir y aplicar políticas de seguridad en base a controles de seguridad establecidos por en las normas internacionales de seguridad de la información para la reducción de riesgo de seguridad.
- Las políticas de seguridad de la información deben ser desarrolladas de acuerdo a las necesidades y requerimientos de la organización, siguiendo los lineamientos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Para futuras investigaciones sobre malas prácticas de seguridad es recomendable definir una metodología que abarque la problemática desde sus causas y consecuencias.
- Antes de la implementación es recomendable que se defina y aplique una normativa de políticas de seguridad formal en base a controles de seguridad que se definen en las normas internacionales, lo que permitirá mantener una mejor gestión del riesgo.

ANEXOS

Anexo 1

Instalación y configuración del ambiente de pruebas

1.1 Características del ambiente de pruebas

La implementación del ambiente de pruebas se hace sobre una laptop que servirá de laboratorio virtual para su desarrollo. De tal forma se implementará la instalación de Windows Server 2016 Standard sobre el software de virtualización VMware, donde se levantarán los servicios de Active Directory con configuraciones y ajustes predeterminados que emulen un escenario de malas prácticas. A continuación, se especifican las características del equipo que se usara para ambiente de pruebas.

1.1.1 Características de Equipo para pruebas

Tabla 22. *Especificaciones de Equipo de pruebas*

Computadora para realizar el ambiente de pruebas	
Hardware	Descripción
Procesador	Intel(R) Core (TM) i5-7500 2.4GHz
Disco duro	1TB SSD
Memoria RAM	8GB 1600MHz
Tarjeta de Red	Realtek PCIe Gabe Familia Controller
Sistema Operativo	Windows 10 Pro x64 bits

Fuente – Información tomada de investigación directa. . Elaborado por el autor

Así mismo se define las características de los recursos que serán asignados a las máquinas virtuales en función de que cumplan los requisitos mínimos para un óptimo desarrollo de las pruebas.

Tabla 23. *Especificaciones de máquina virtual servidor*

Especificaciones de máquinas virtuales.			
Características	**Domain Controller**	**Usuario del dominio**	**Kali Linux**
Procesador	Virtual de 2 núcleos	Virtual de 2 núcleos	Virtual de 2 núcleos
Disco duro	60 GB	60 GB	60 GB
Memoria RAM	2 GB	1GB	1GB
Tarjeta de Red	Realtek PCIe GbE Familia Controller - virtual	Realtek PCIe GbE Familia Controller - virtual	Realtek PCIe GbE Familia Controller – virtual

Fuente – Información tomada de investigación directa. . Elaborado por el autor

Características de Software

Tabla 24.*Requisitos de Software.*

Software necesario para generar el ambiente de pruebas	
Software	Versión
VMware Workstation	16 pro x64 bits
Windows 10	Pro x64 bits
Windows Server	2016 x64 bits
Kali Linux	2021.1

Fuente – Información tomada de investigación directa. . Elaborado por el autor

1.2 Configuración del ambiente de pruebas

1.2.1 Instalación de VMware

a) Inicio de instalación de VMware

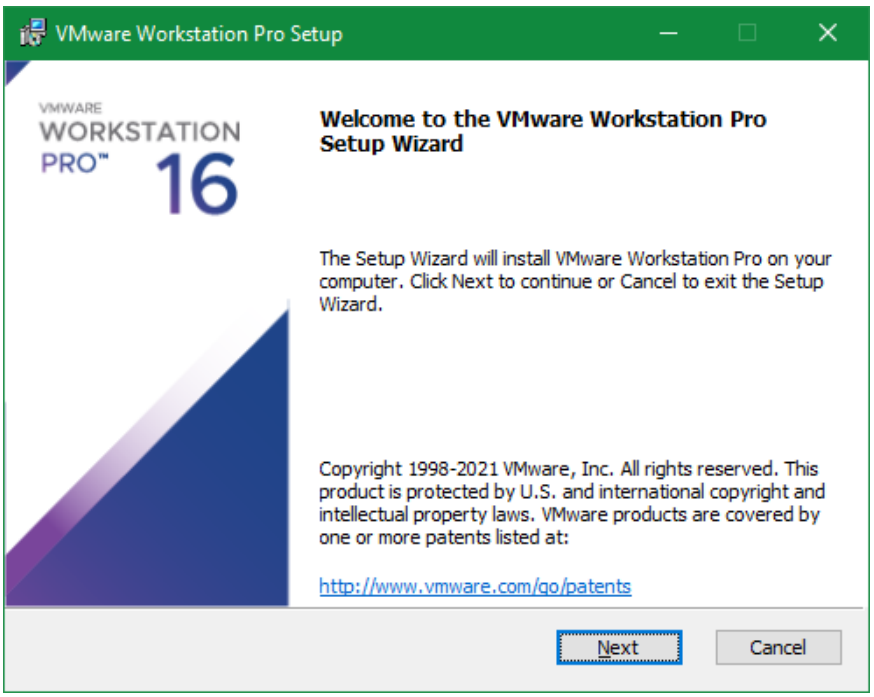


Figura 28*.Insstalacion de VMware. Elaborado por el autor.*

b) Aceptación de términos y condiciones de uso.

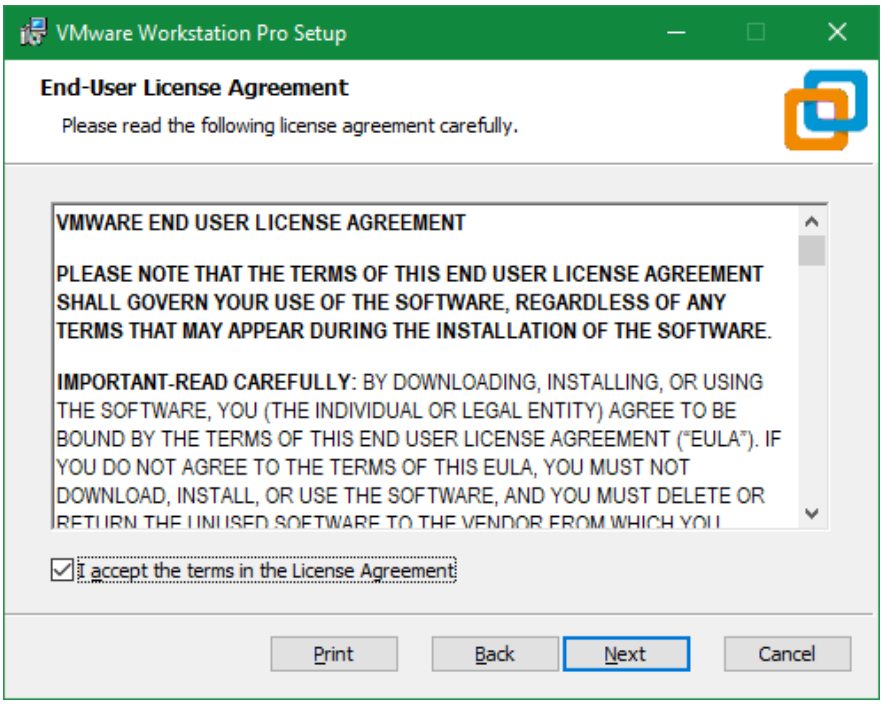


Figura 29. *Aceptación de términos y condiciones en VMware. Elaborado por el autor.*

c) Selección del destino de instalación

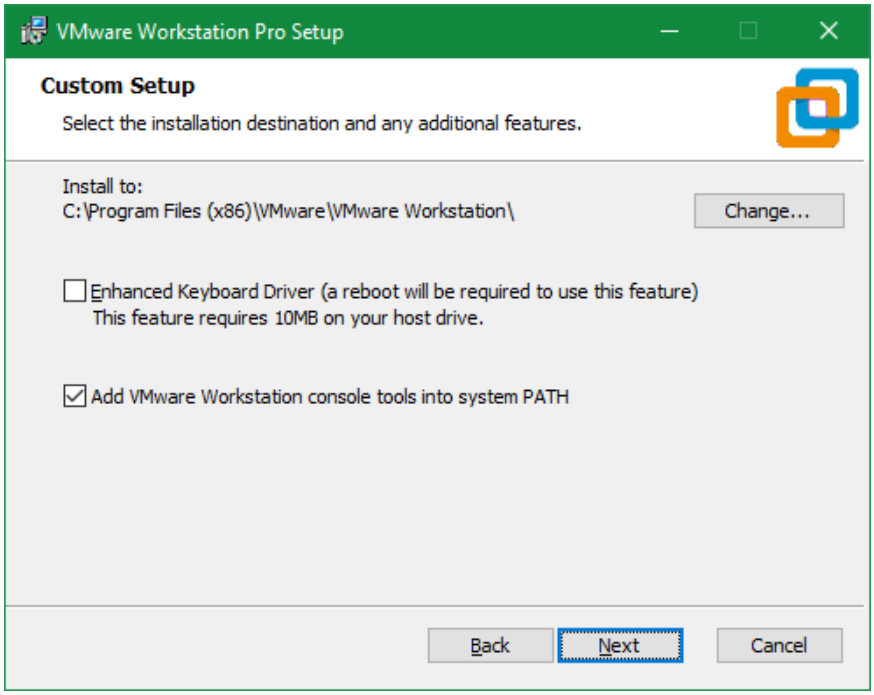


Figura 30. *Selección de destino de instalación de VMware. Elaborado por el autor*

d) Proceso de instalación de VMware

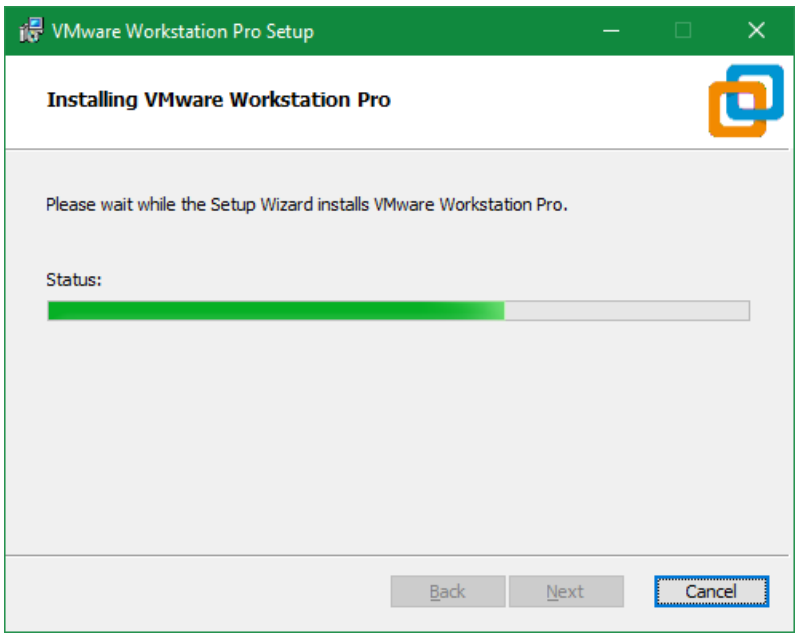


Figura 31. *Proceso de instalación de VMware. Elaborado por el autor.*

e) Ejecución de VMware.

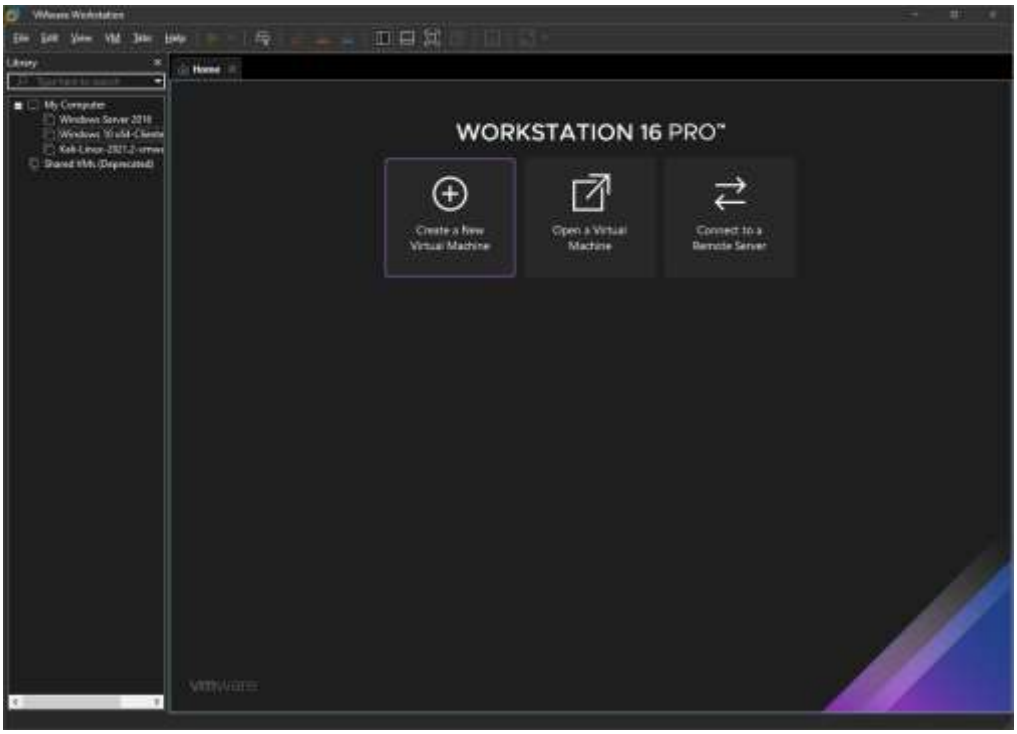


Figura 32. *Ejecución de VMware. . Elaborado por el autor*

1.3 Instalación de máquinas virtuales

1.3.1 Como crear una máquina virtual

A continuación, se detallan los pasos para crear una máquina virtual en el software de virtualización VMware Workstation 16 Pro.

1) En el panel principal de VMware se elige “Create a New Virtual Machine” (Crear una nueva máquina virtual).

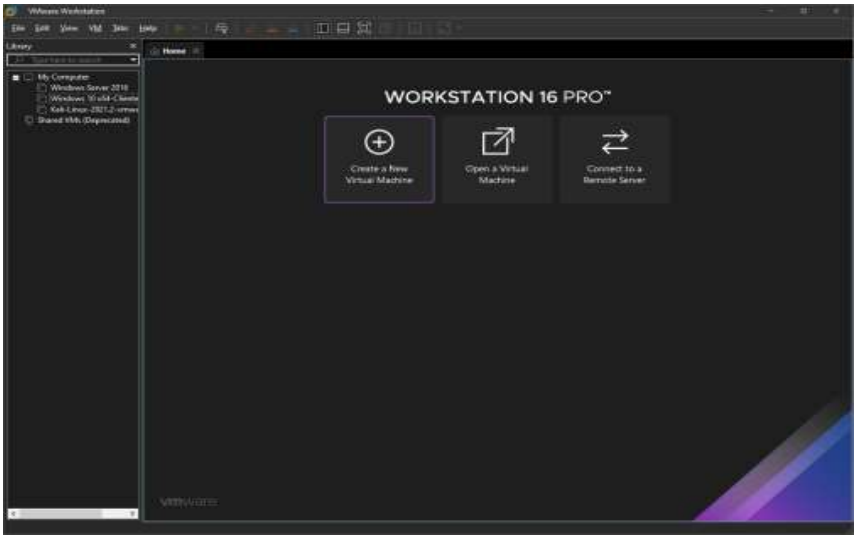


Figura 33*.Opción crear nueva máquina virtual. Elaborado por el autor*

2) Después de elegir esta opción se despliega la ventana para elegir el origen del software del sistema operativo a instalar. En este caso se utiliza la imagen ISO del Sistema Operativo Windows Server 2016 Standard previamente descargado de la web.

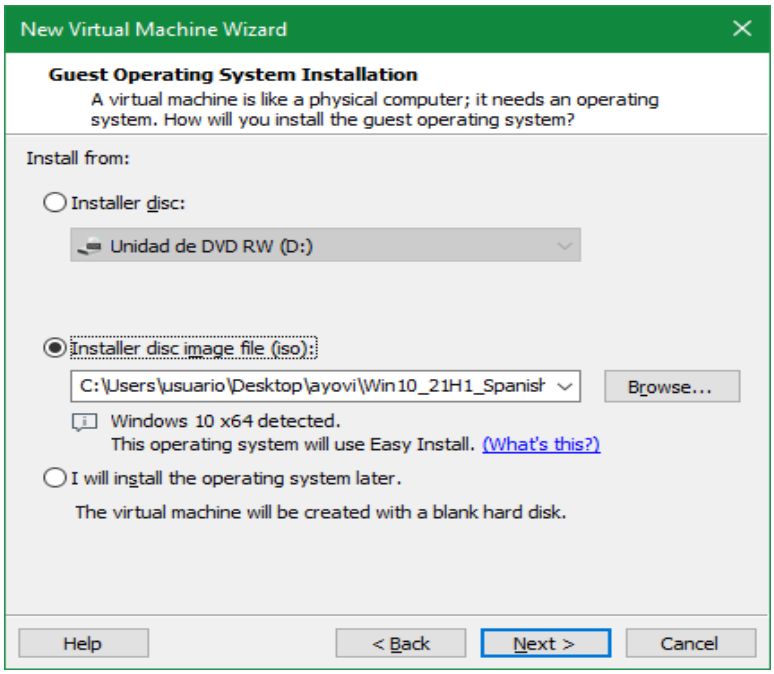


Figura 34 *Elección de imagen ISO. Elaborado por el autor*

3) Se despliega la ventana de personalización donde se podrá definir el nombre del inicio de sesión en el sistema operativo y su contraseña. En este caso se deja por defecto los parámetros de personalización.

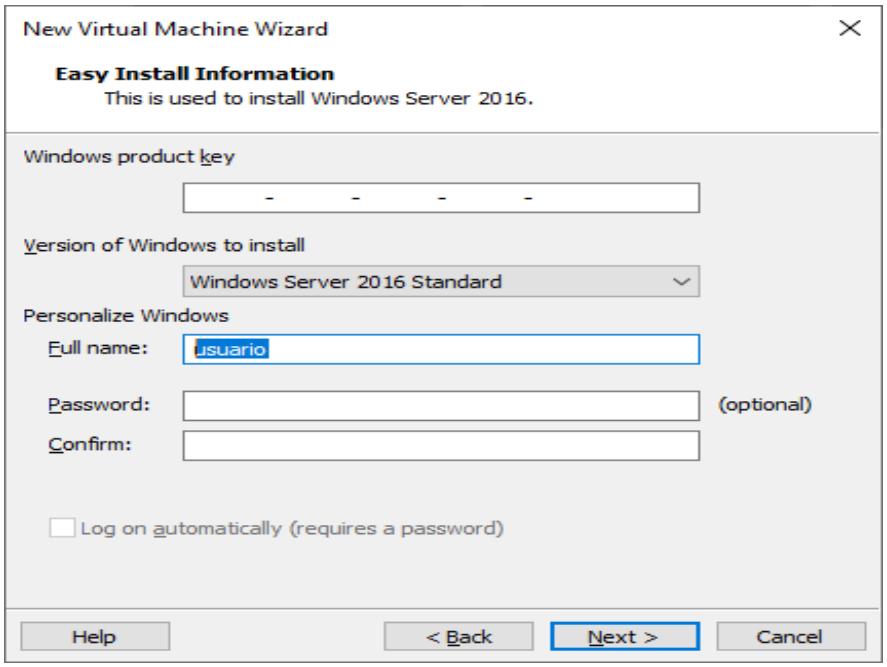


Figura 35. *Personalización de inicio de sistema. Elaborado por el autor.*

4) Elegir el nombre de la máquina virtual y la ubicación de la misma en el disco duro.

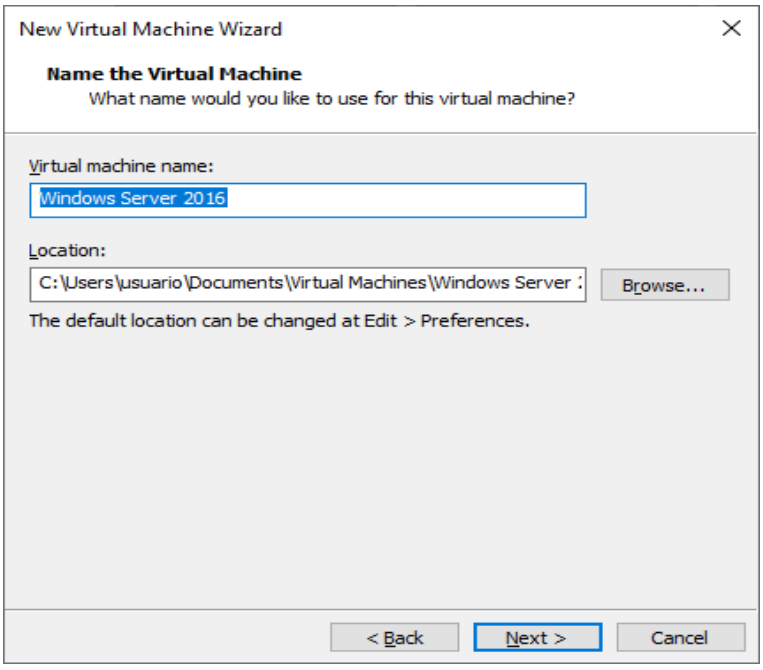


Figura 36*. Nombre y ubicación de máquina virtual. . Elaborado por el autor*

5) Seleccionar el tipo de Firmware de lectura.

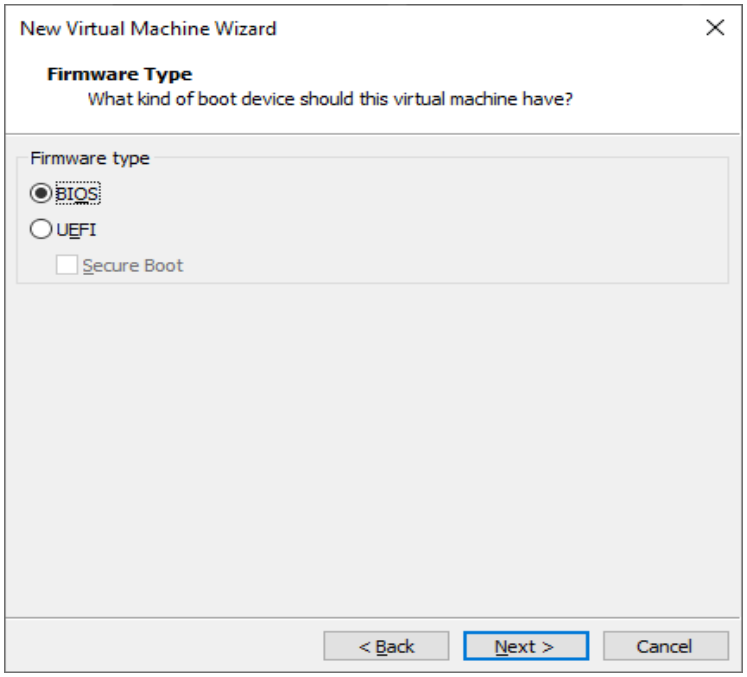


Figura 37. *Selección de Tipo de Firmware. Elaborado por el autor*

6) Elegir el número de procesadores.

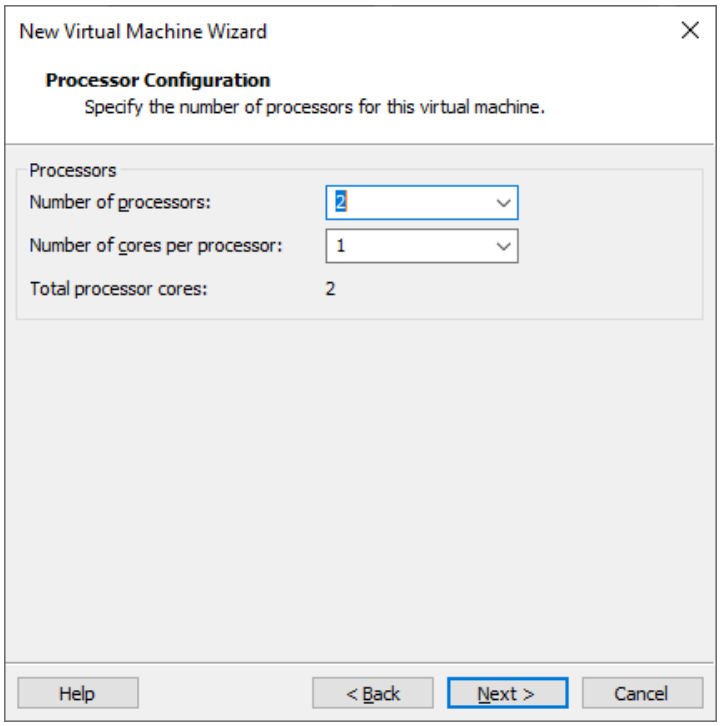


Figura 38. *Elección de número de procesadores. Elaborado por el autor.*

7) Elegir la cantidad de memoria de virtualización tomada de la memoria RAM.

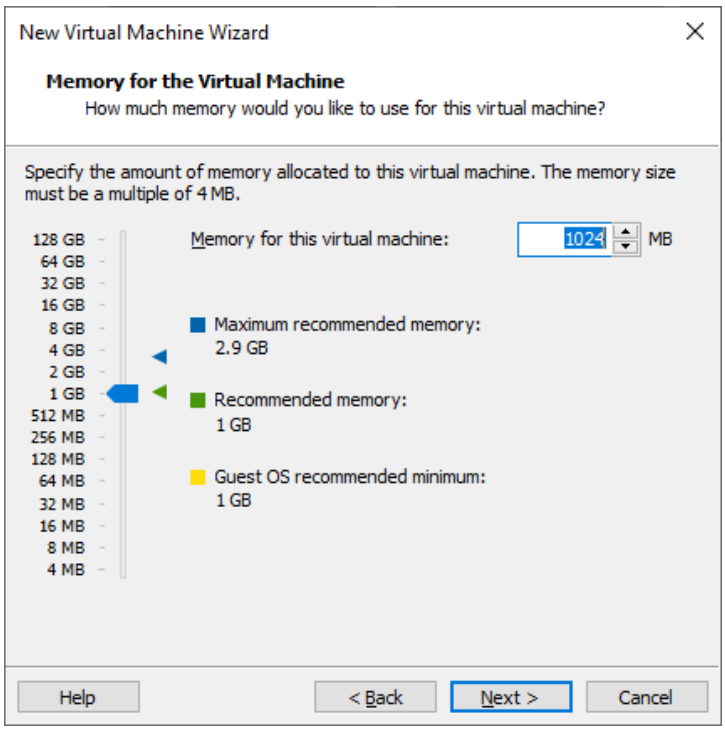


Figura 39. *Elección de memoria virtual. Elaborado por el autor.*

8) Seleccionar el tipo de conexión de red, el cual puede ser:

- NAT. - Utiliza la conexión del equipo para navegar en internet
- Bridge: Realiza un puente con la tarjeta de red asumiendo una configuración de red local sin acceso a internet.
- Host: Utiliza el equipo anfitrión como host de una red privada
- Sin conexión

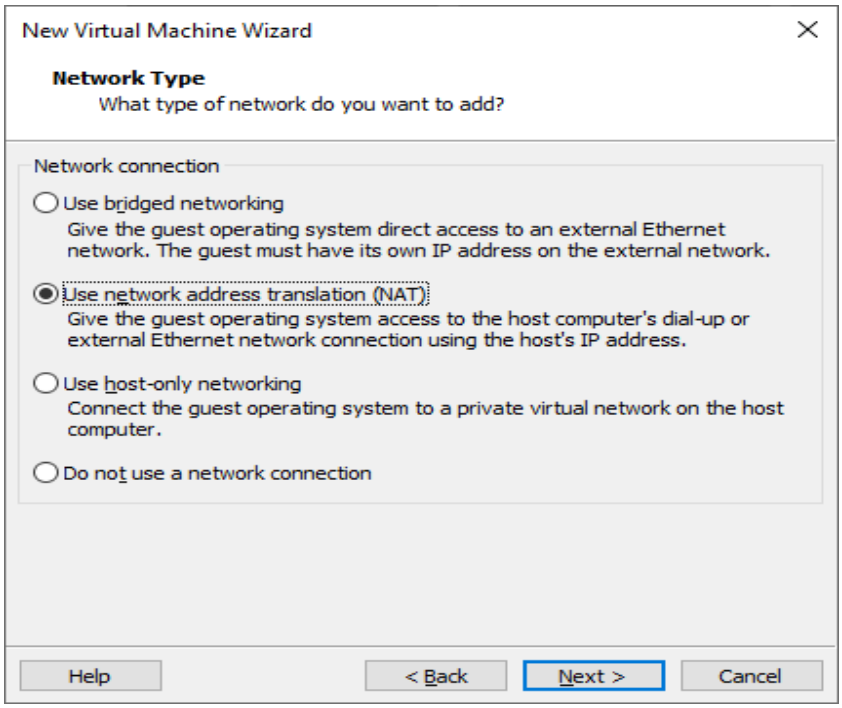


Figura 40. *Selección de tipo de conexión de red. Elaborado por el autor.*

9) Elegir el tipo de disco duro a usar

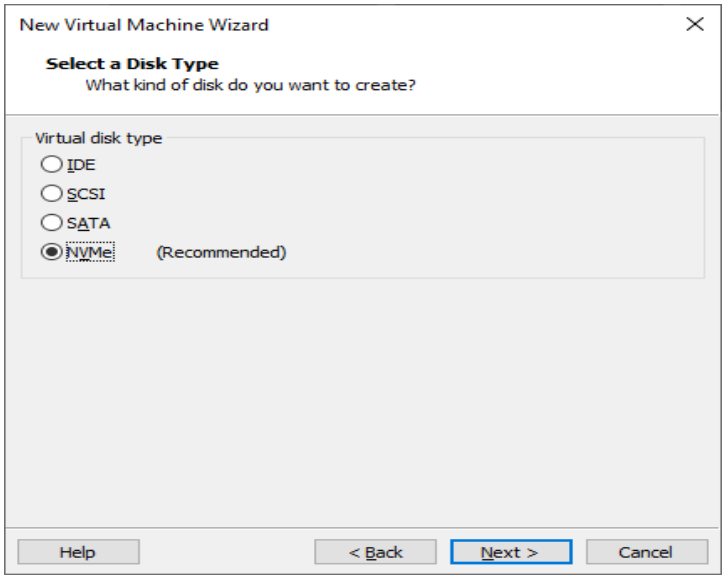


Figura 41. *Elección del tipo de disco duro. Elaborado por el autor.*

10) Seleccionar el disco a utilizar

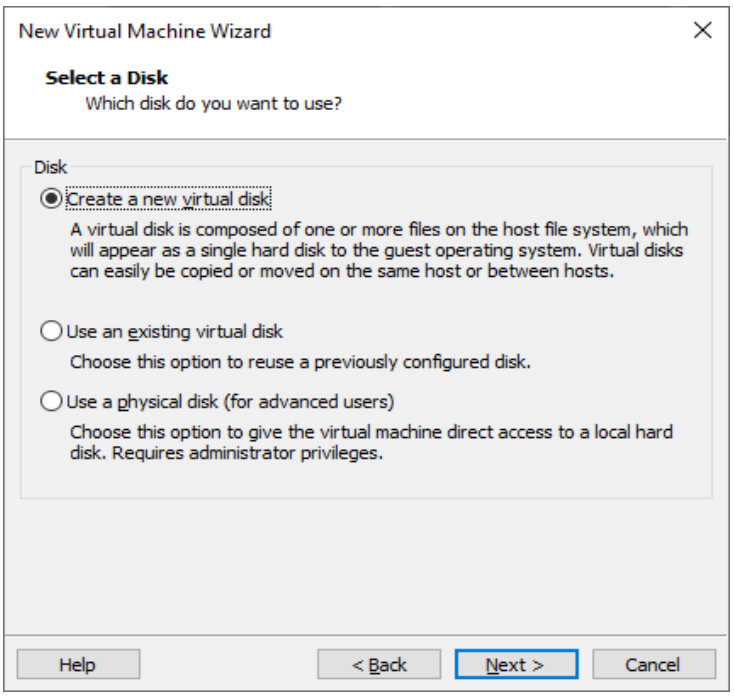


Figura 42. *Selección de disco duro a usar. Elaborado por el autor.*

11) Especificar la capacidad del disco duro de la máquina virtual.

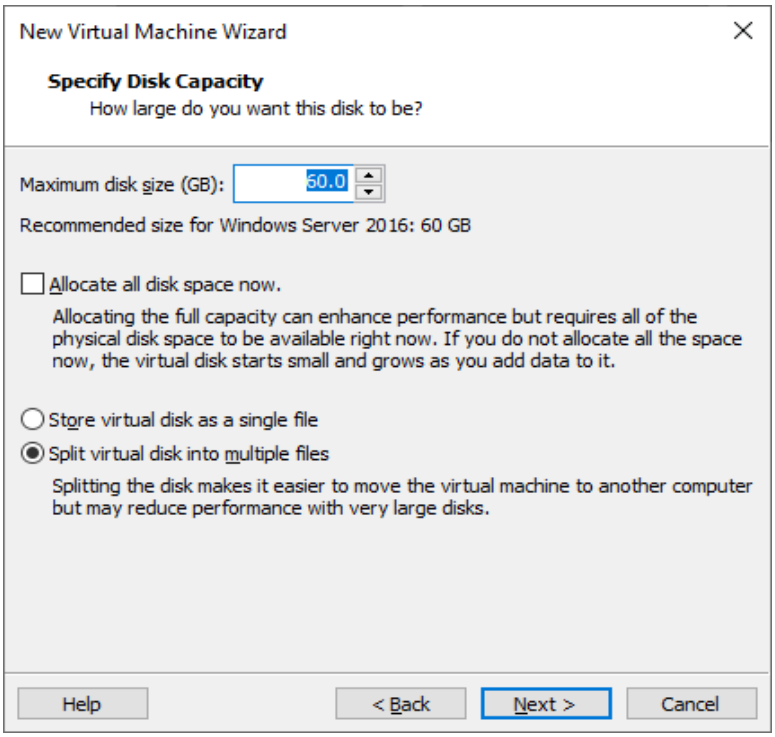


Figura 43. *Especificación de capacidad de disco duro. Elaborado por el autor.*

12) Verificar de las características y configuraciones seleccionadas para la nueva máquina virtual y finalizar.

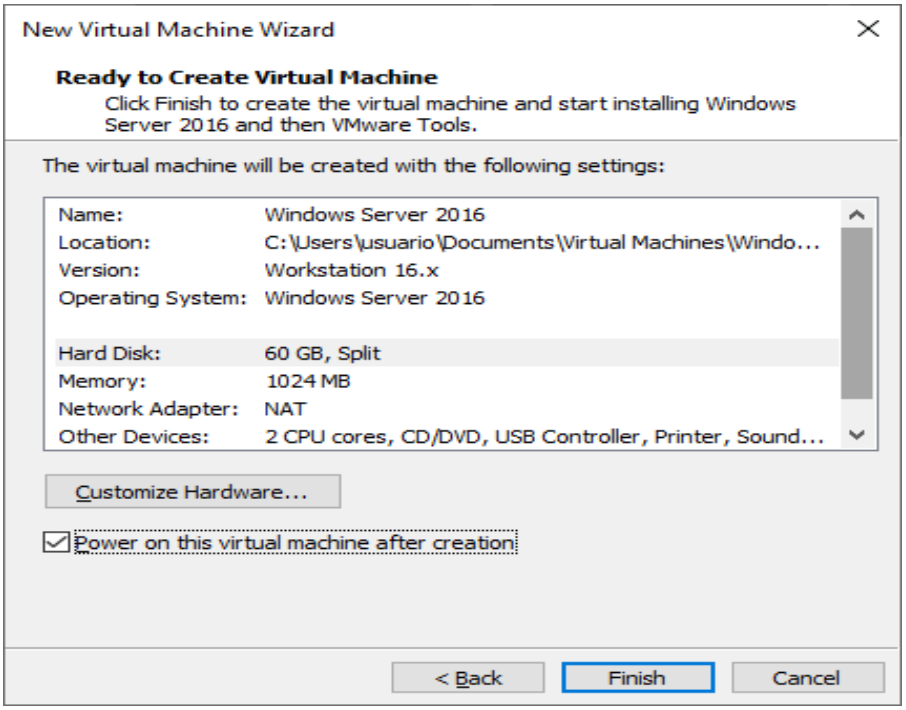


Figura 44. Revisión de características elegidas. Elaborado por el autor

1.3.2 Instalación de Windows Server 2016

1) Inicializar máquina virtual y arrancar el sistema operativo de Windows Server 2016

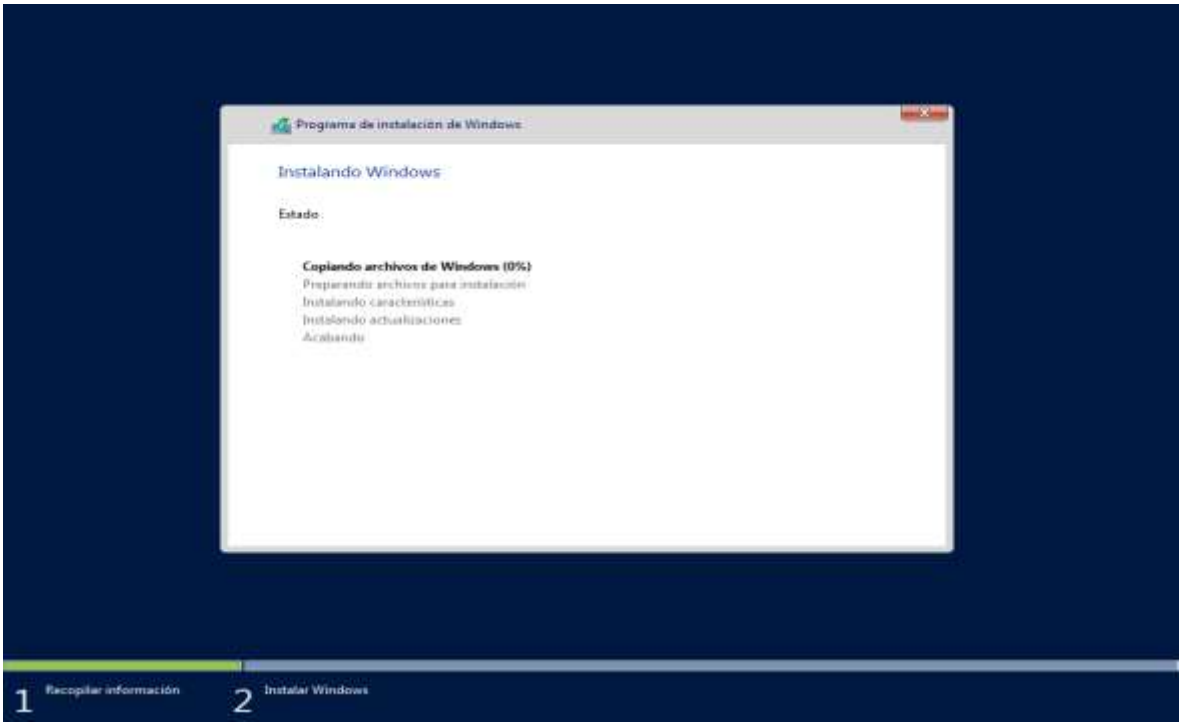


Figura 45*. Instalación de Windows Server 2016. Elaborado por el autor.*

2) Sistema instalado e iniciado.

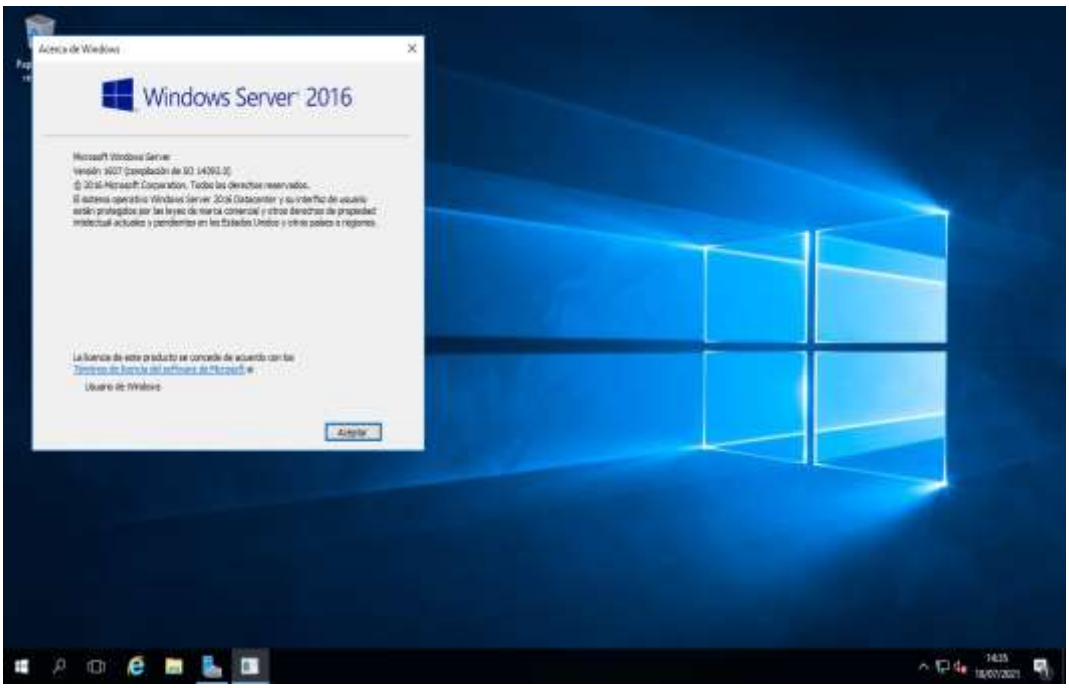


Figura 46.*Inicio de Windows Server 2016.Elabrado por el autor*

1.3.3 Instalación de Windows 10 Pro

1) Inicializar la máquina virtual para Windows 10 y elegir la versión del sistema a instalar.

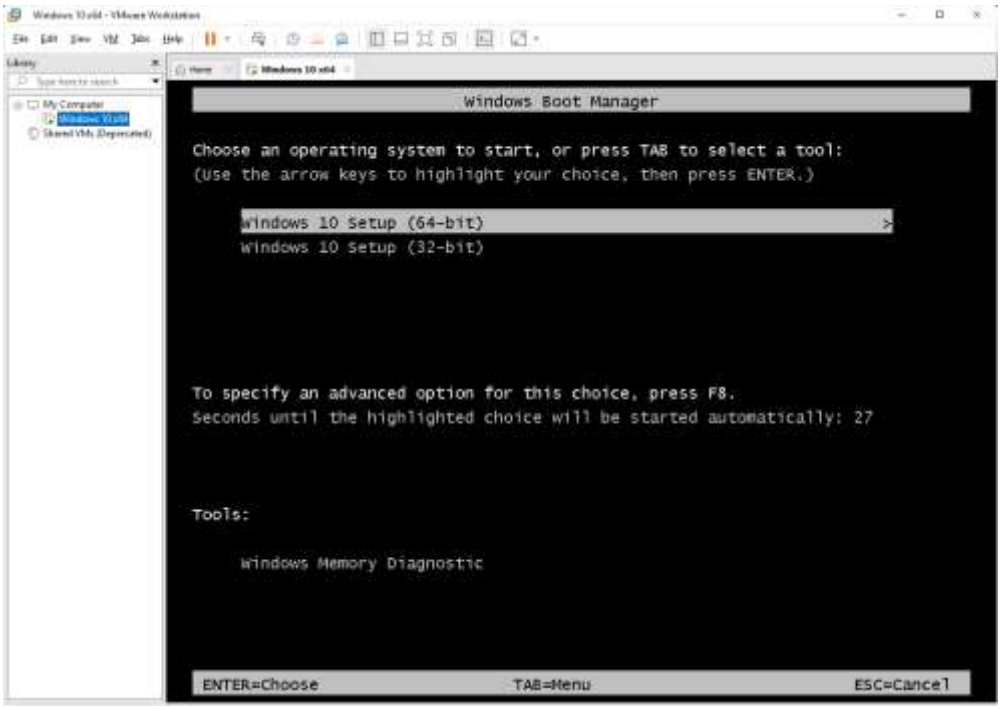


Figura 47. *Inicialización de máquina virtual de Windows 10. . Elaborado por el autor*

2) Instalación de Windows 10 en máquina virtual.

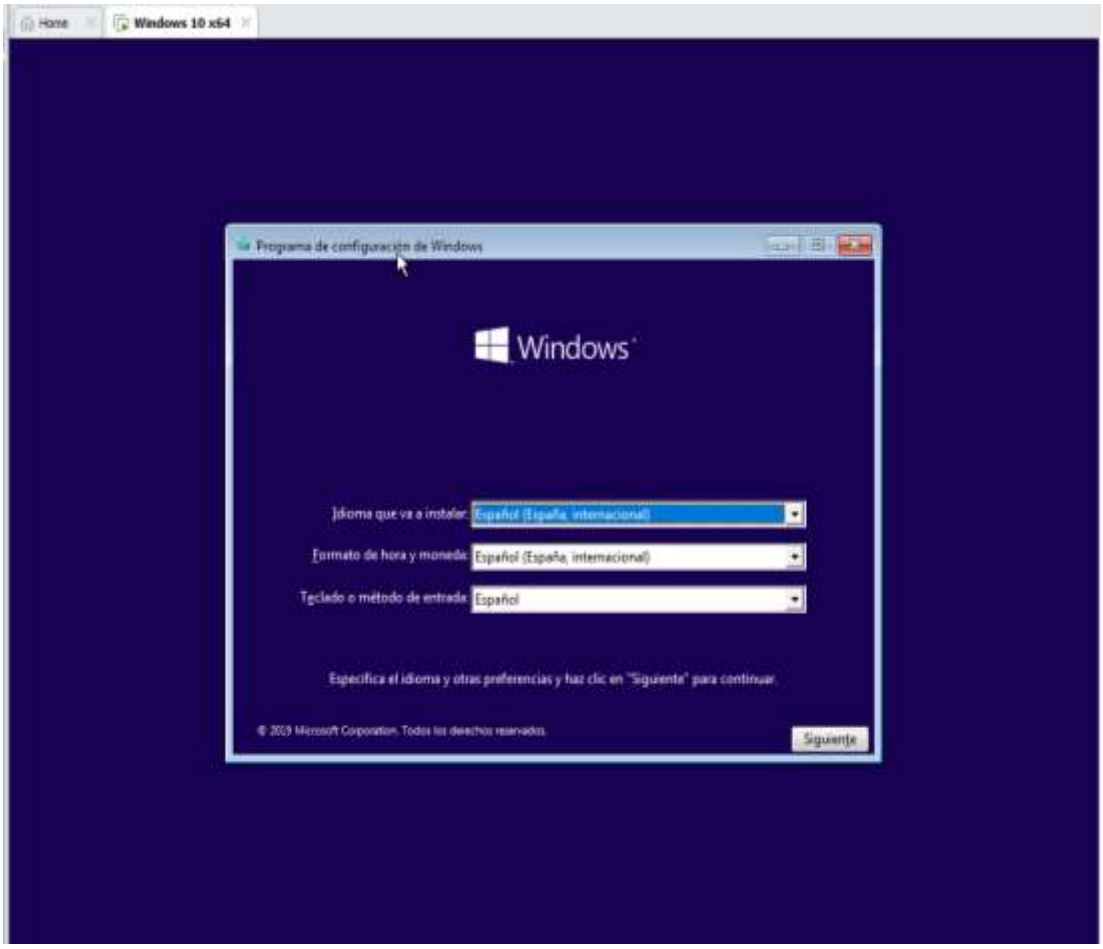


Figura 48.Instalacion de Windows 10. Elaborado por el autor.

3) Inicio de Windows 10 en máquina virtual.

Figura 49. *Inicio de Windows 10. Elaborado por el autor.*

1.3.4 Instalación de Kali Linux

1) Inicio de máquina virtual e instalación de Kali Linux.

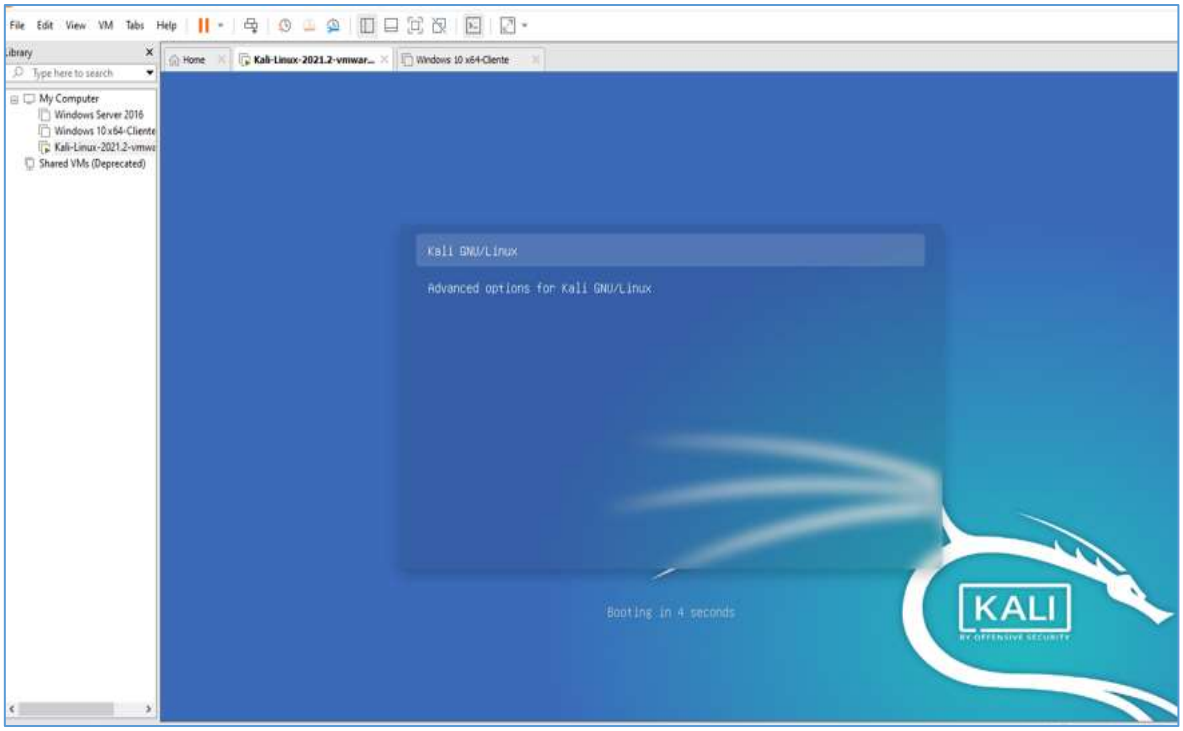


***Figura 50**. Inicio de Kali Linux. Elaborado por el autor.*

2) Inicio Kali Linux

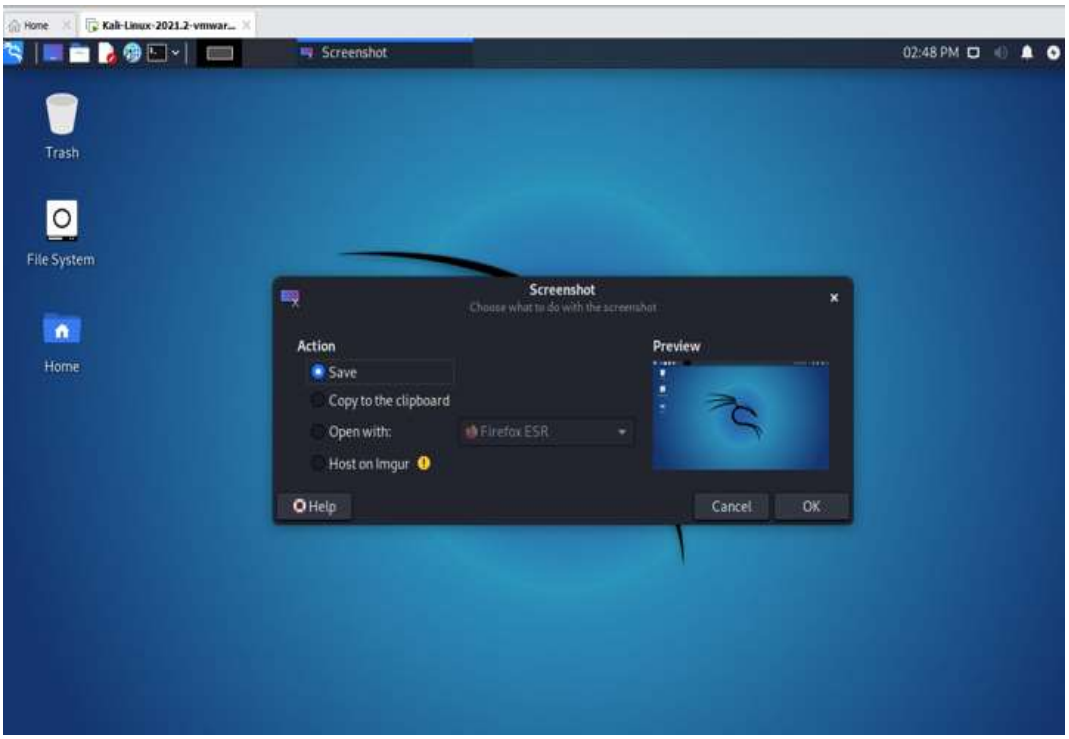


***Figura 51**.Inicio de Kali Linux. . Elaborado por el autor*

1.4 Instalación y configuración de Active Directory con malas prácticas

Después de la implementación del sistema operativo Windows Server, se procede con la instalación de los servicios de Active Directory, en base a las malas prácticas de seguridad que han sido investigadas

1.4.1 Configuración del hostname identificable

Dentro del administrador del servidor, se inician las propiedades del servidor local y se cambia el nombre del equipo a DC-GYE.

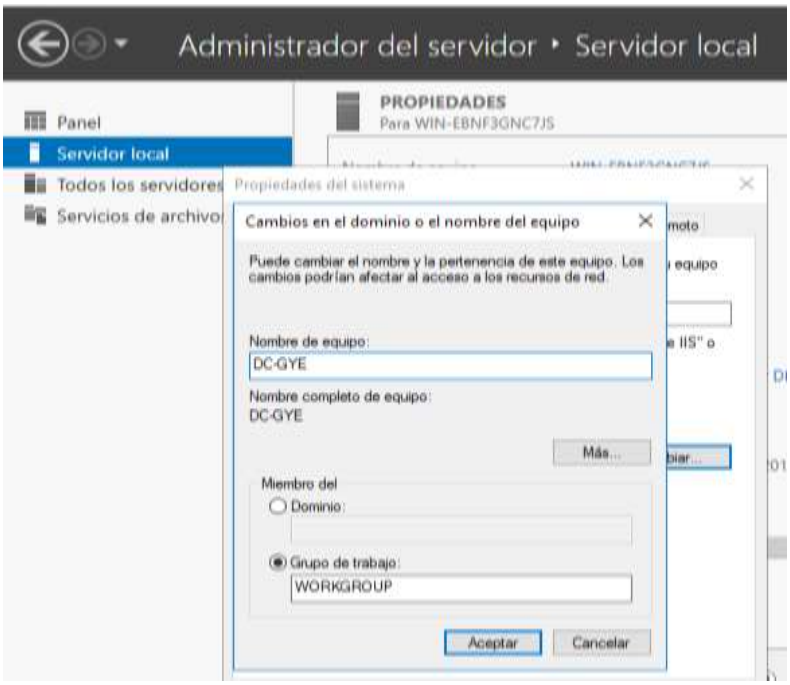


***Figura 52**.Configuracion de Hostname. Elaborado por el autor*

1.4.2 Instalación de los servicios de Active Directory con malas practicas

1.4.2.1 *Configuración de única red local.*

***Tabla 25**.Ajuste de red del servidor de Active Directory*

Red local	**DC-GYE**
IP	192.168.109.130
Mascara de red	255.255.255.0
Puerta de enlace	192.168.109.2
DNS	127.0.0.1

Fuente tomada de investigación directa. Elaborada por el autor

1) **Configuración de dirección IP, Mascara de red y Puerta de enlace en el equipo servidor.**

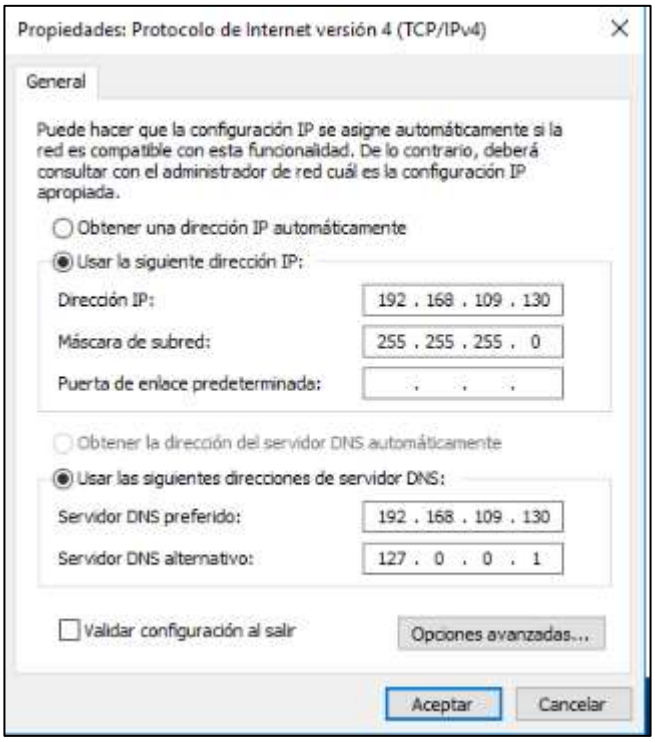


Figura 53. *Configuración de la red local del servidor. Elaborado por el autor.*

2) **Comprobación de configuración de la red local.**

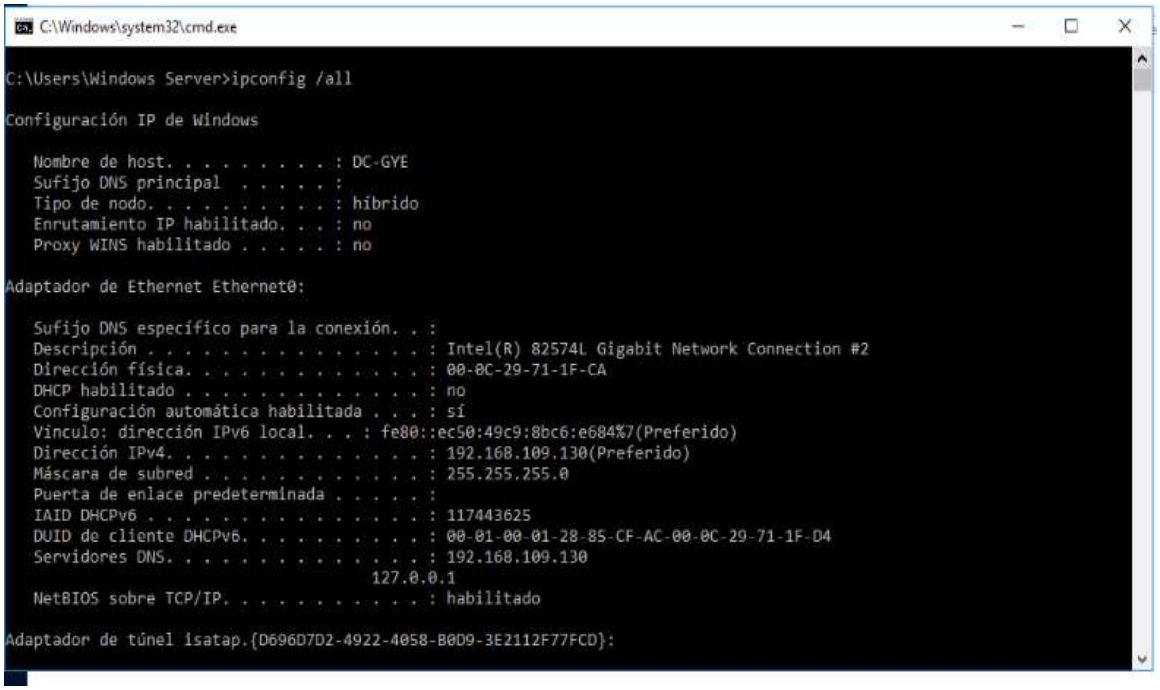


Figura 54.*Comprobación de la red local. Elaborado por el autor*

1.4.2.2 Instalación de roles y características

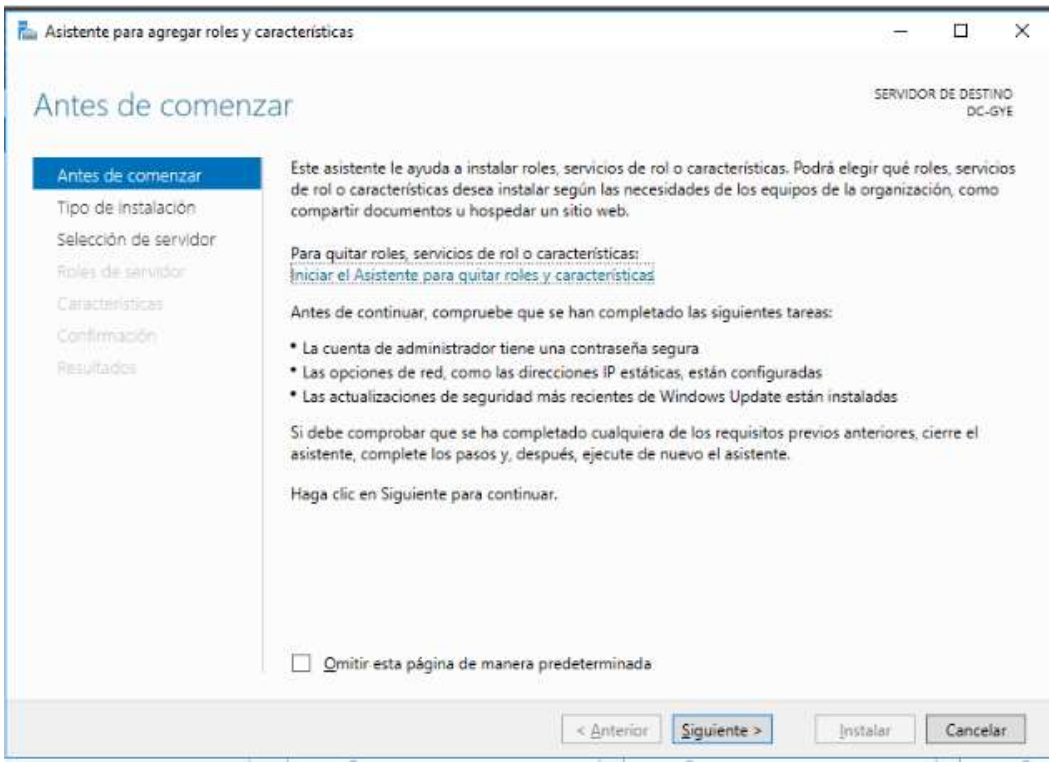


Figura 55. *Instalación de Roles y Características del servidor. . Elaborado por el autor*

1) Selección de un solo servidor de Active Directory, sin otro de respaldo

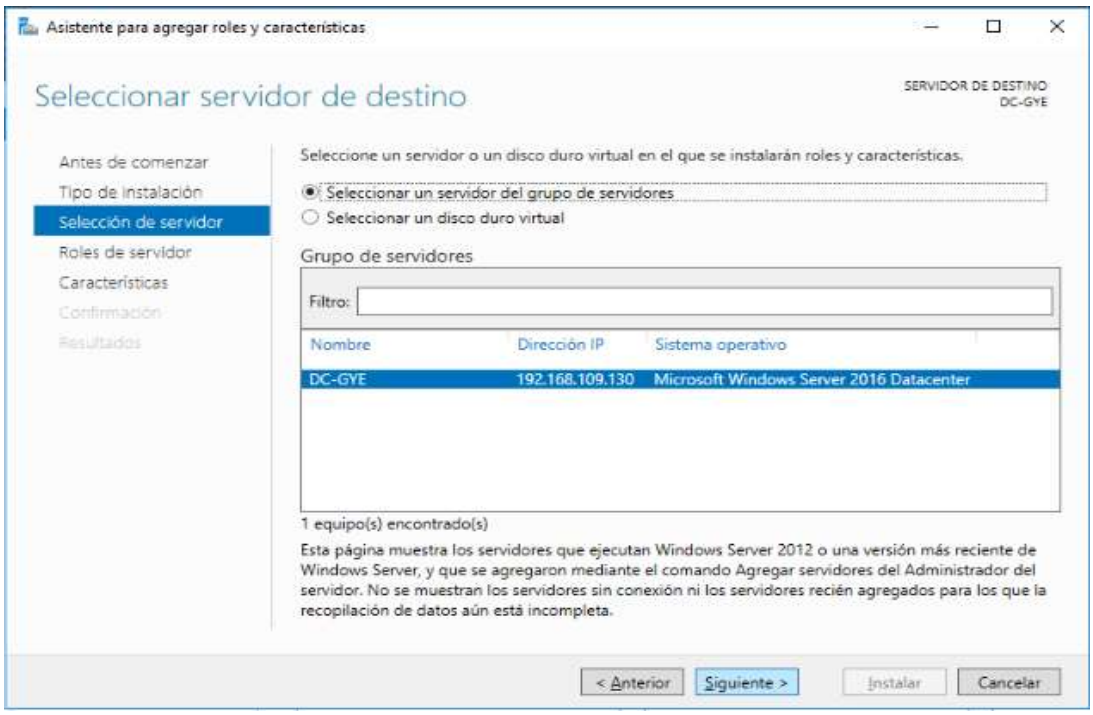


Figura 56*.Servidor de destino. Elaborado por el autor*

2) Selección de roles del servidor por defecto

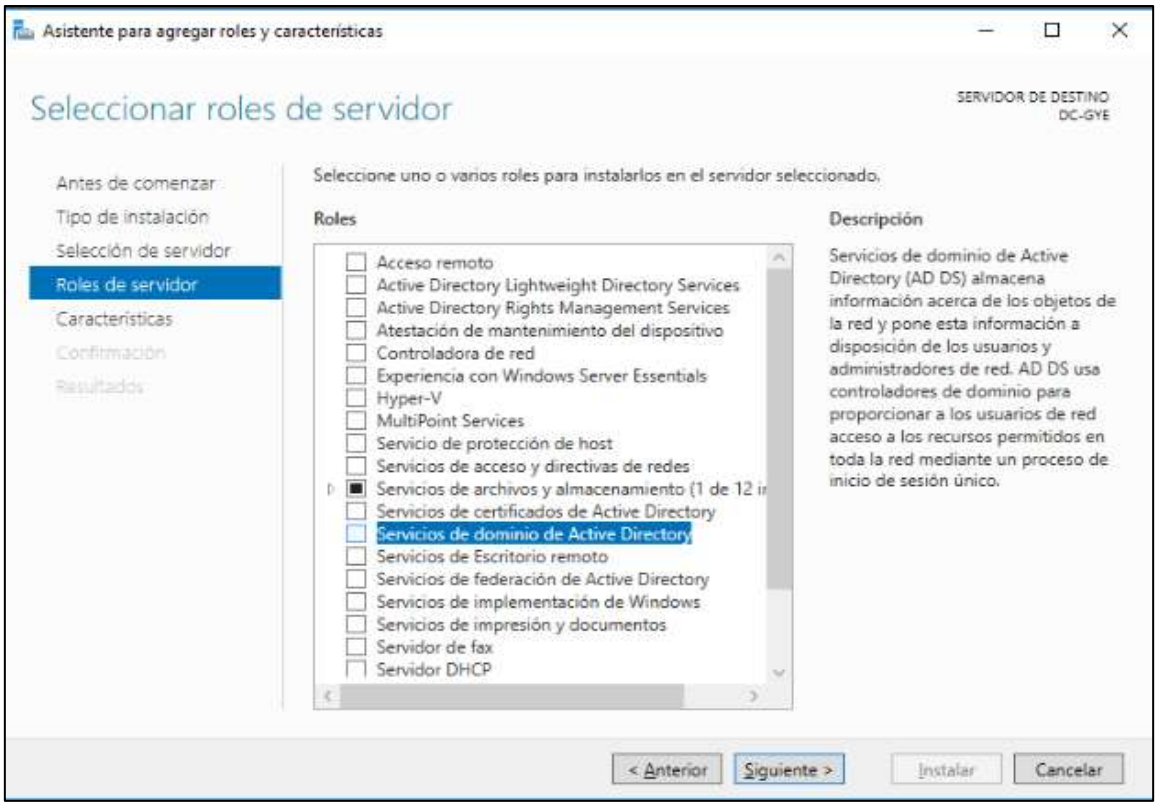


Figura 57. *Ajuste de roles de servidor de Active Directory. Elaborado por el autor*

3) Levantamiento de los servicios Azure Active Directory

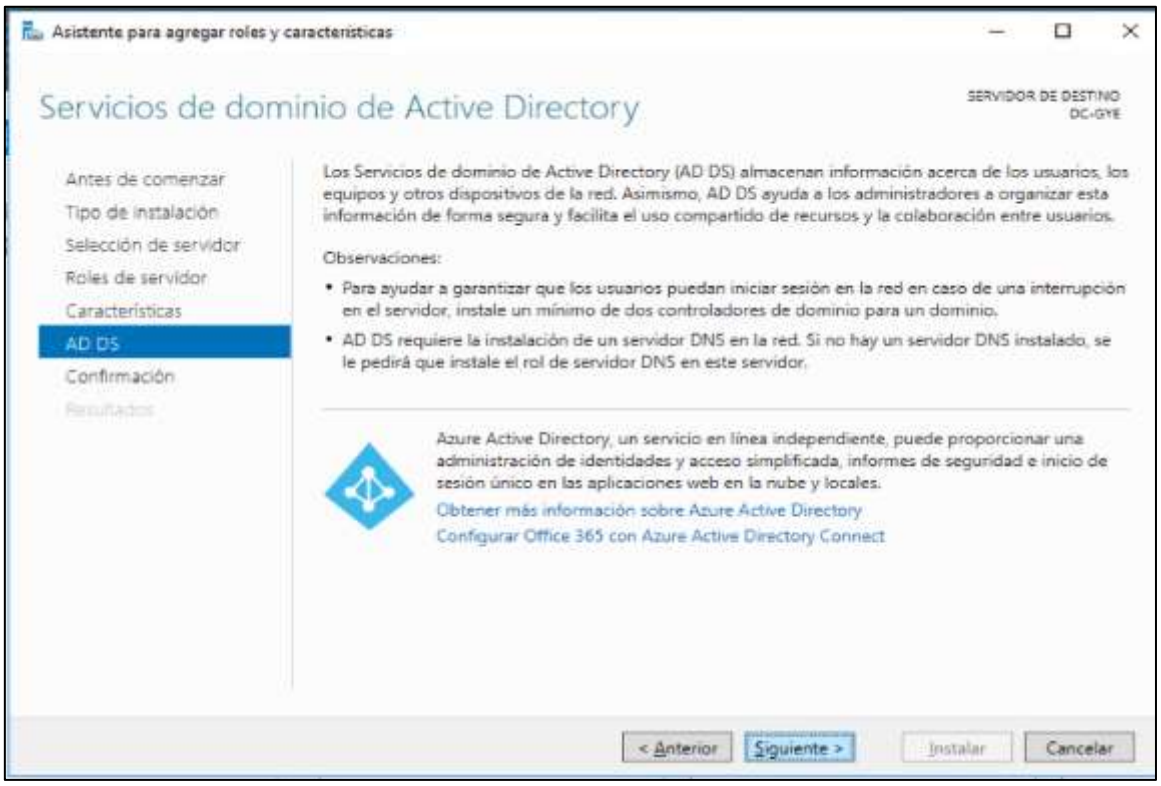


Figura 58*.Servicios Azure Active Directory. Elaborado por el autor.*

4) Proceso de instalacion de Active Directory sin verificacion de las caracterisiticas.

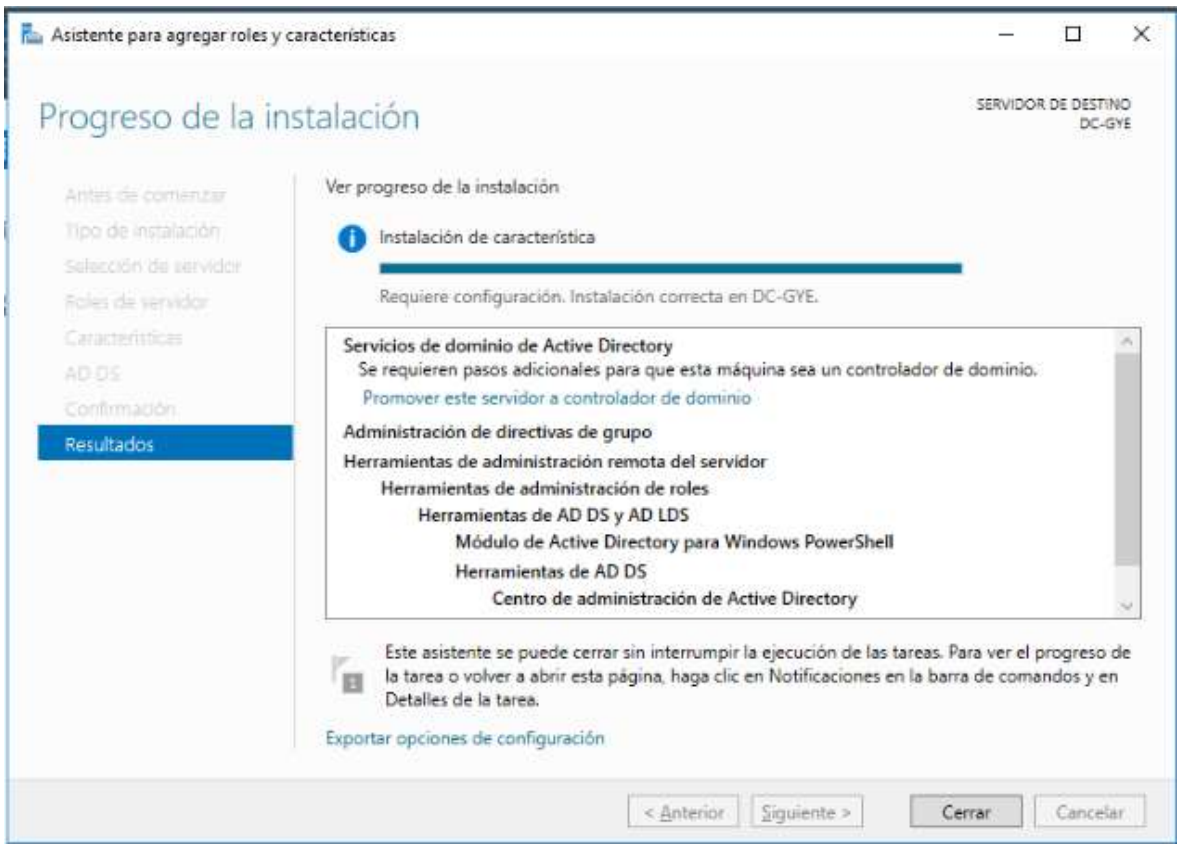


Figura 59.*Proceso de Instalación de Active Director*

1.4.3 Configuración de active Directory con malas practicas

Promoción del servidor a Domain Controller.

1) Crear un nuevo bosque raiz

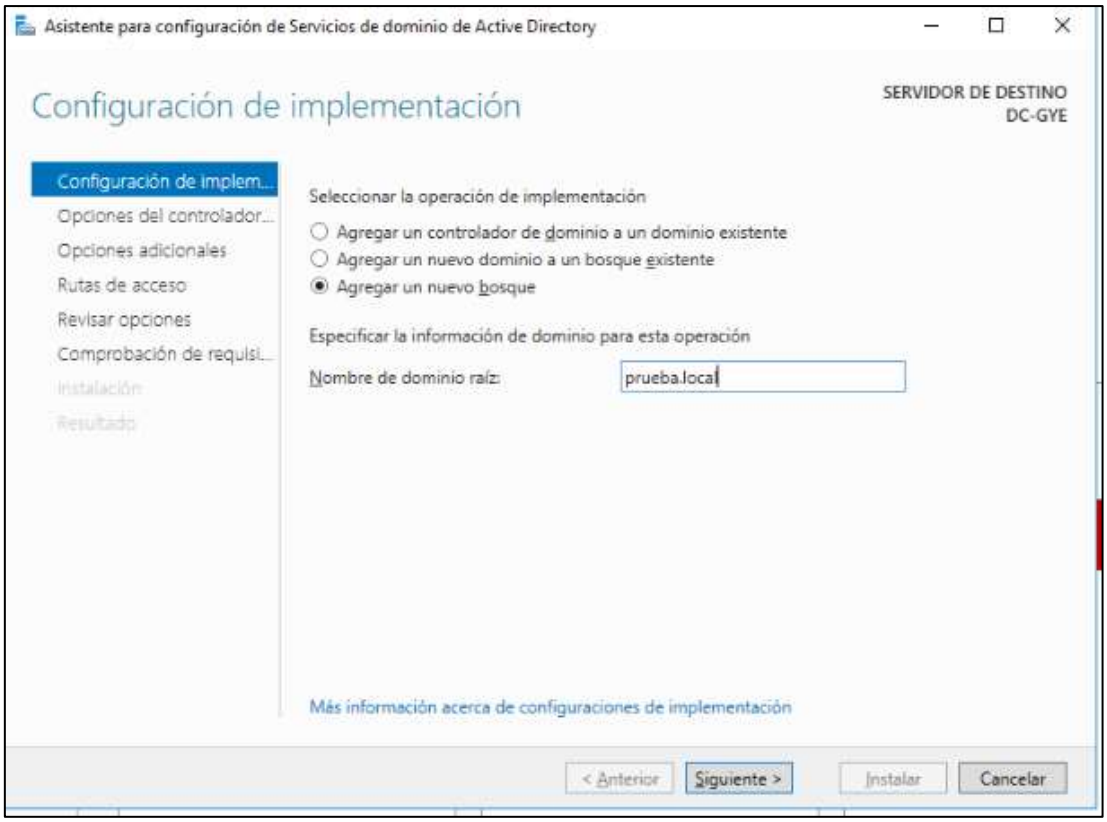


Figura 60. *Creación de nuevo bosque raíz. . Elaborado por el autor*

2) Promoción a catalogo global y activación de servicios DNS sin delegación a otro servidor.

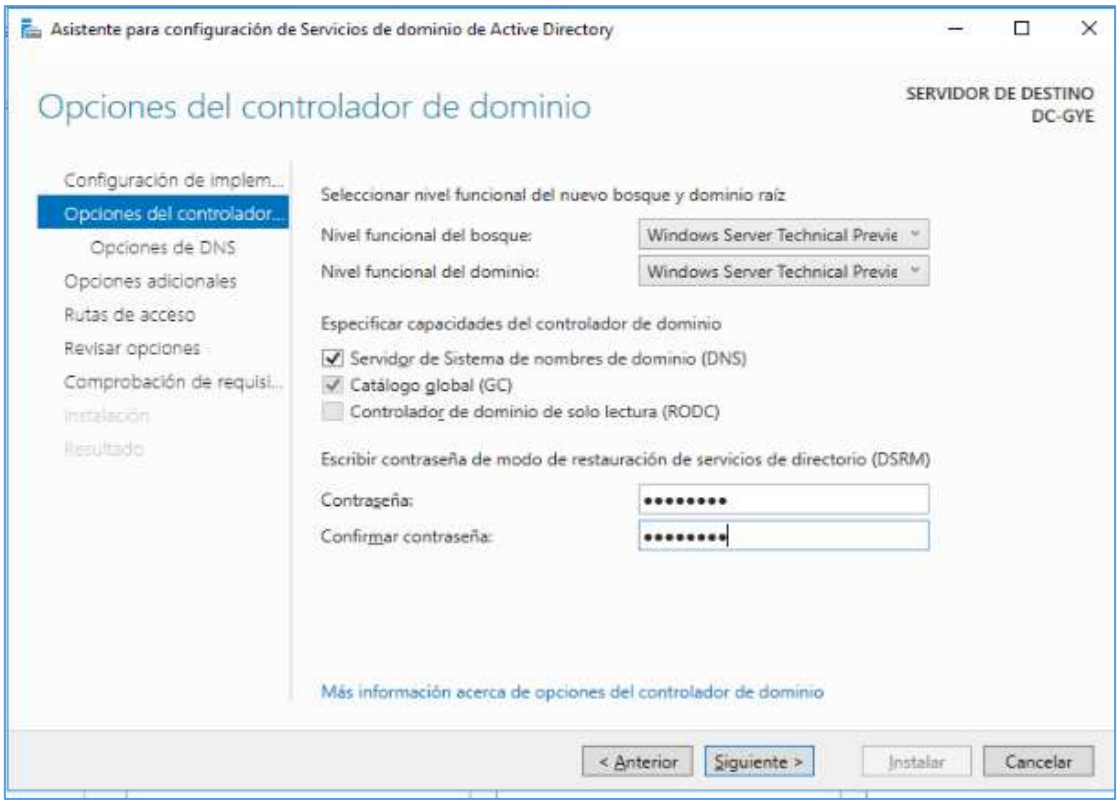


Figura 61. *Promoción del servidor y Activación de DNS*

3) Configuración de rutas de bases de datos, registros y SYSVOL en una sola unidad de disco.

Figura 62*. Dirección de almacenamiento de Active Directory. Elaborado por el autor*

4) Comprobación de requisitos previos

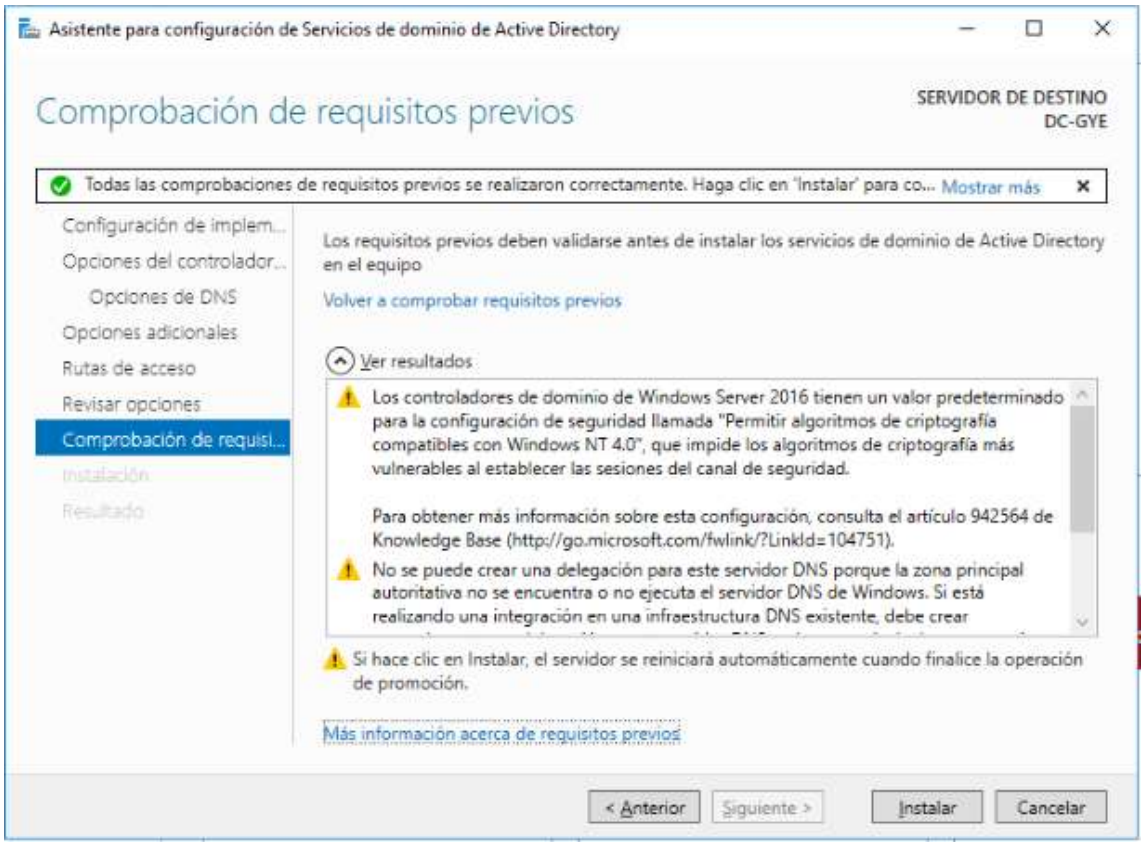


Figura 63. *Comprobación de requisitos. Elaborado por el autor*

5) Inicio de Sesión del controlador de dominio

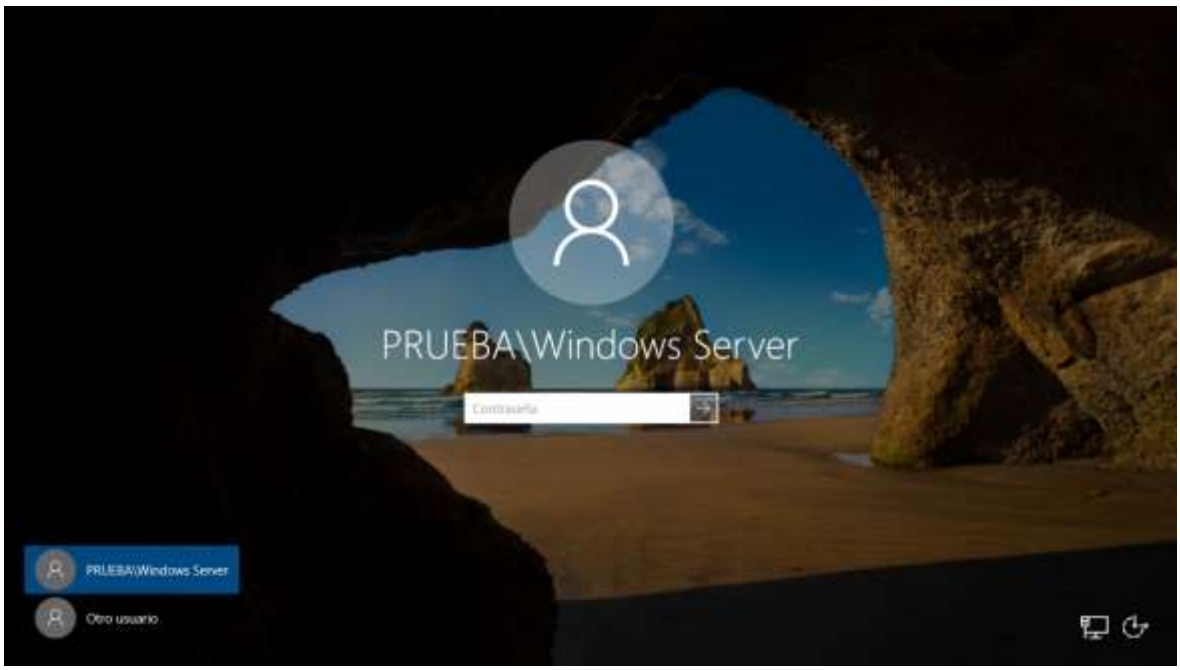


Figura 64.*Inicio de sesión Domain Controller. Elaborado por el autor*

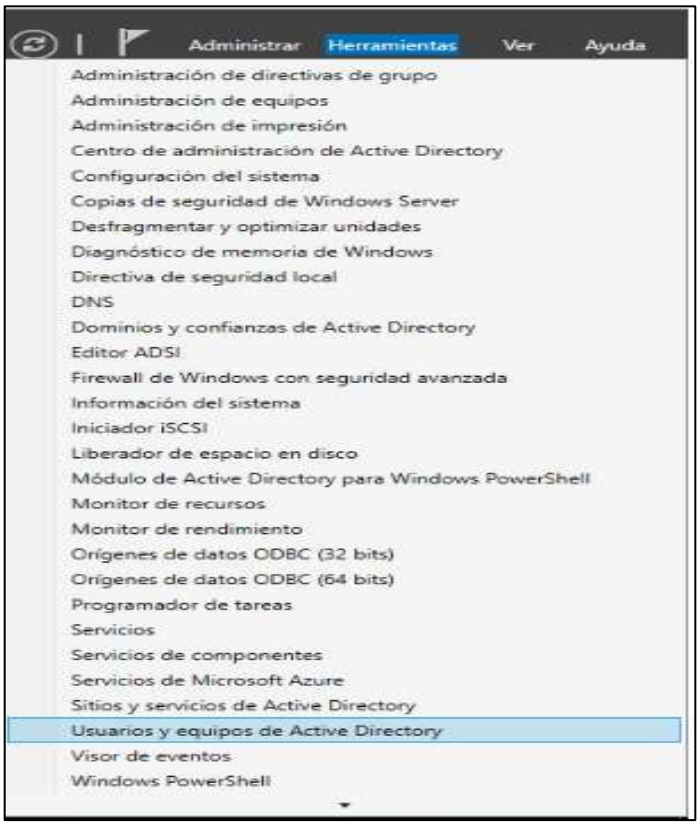
6) Comprobación de los servicios activos en el panel de propiedades

Figura 65. *Propiedades del servidor de Active Directory. Elaborado por el autor*

1.4.4 Creación de Unidades Organizativas y usuarios.

Crear unidades Organizativas

1) Selección de la herramienta Usuarios y Equipos de Active Directory



Figuran 66. *Herramienta Usuarios y Equipos. Elaborado por el autor*

2) Agregar nueva unidad Organizativa al catálogo global

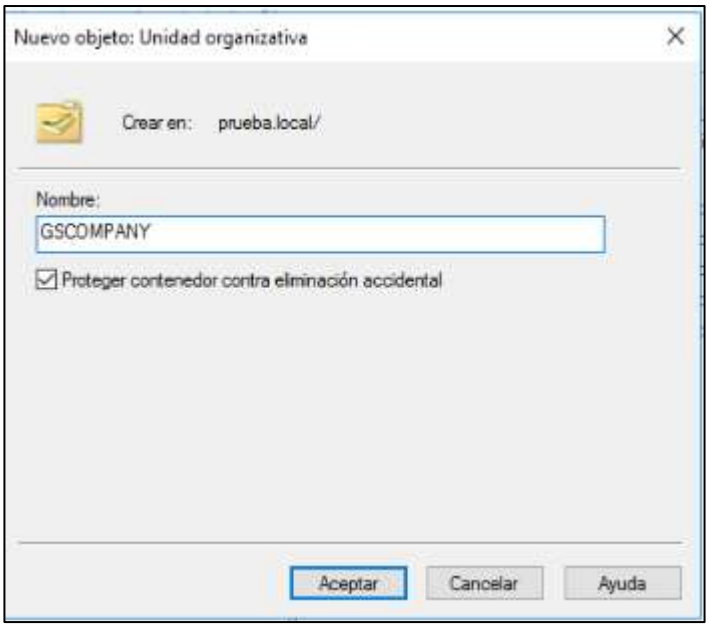


Figura 67*. Nueva Unidad Organizativa. Elaborado por el autor*

Crear Unidades Organizativas internas

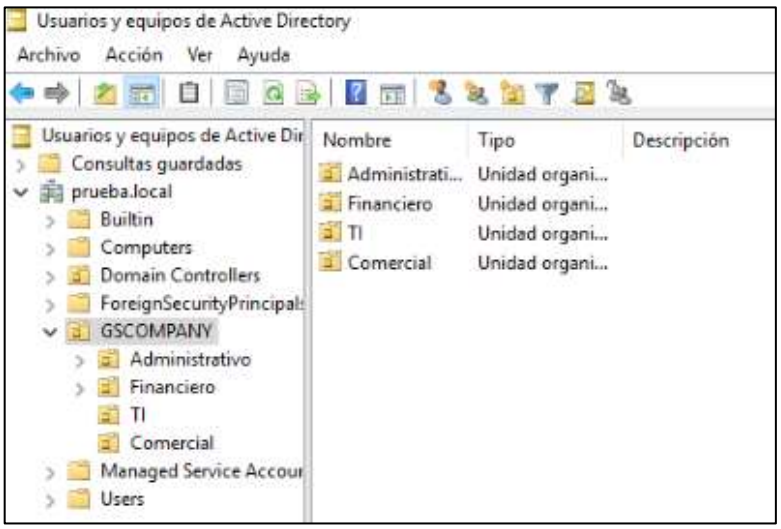


Figura 68. *Creación de Unidades Organizativa internas. Elaborado por el autor*

Crear usuarios del dominio

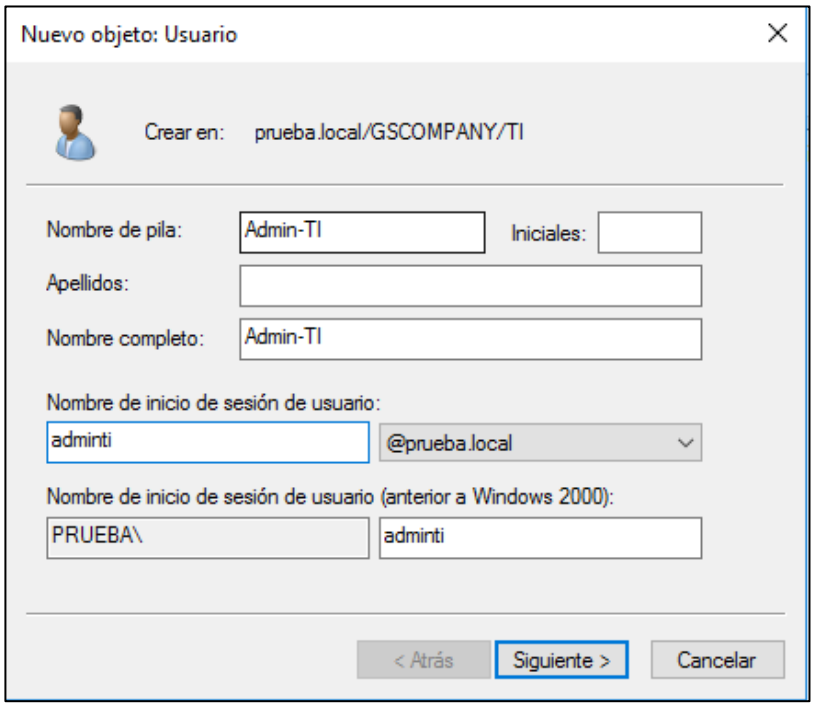


Figura 69.*Creacion de usuarios del dominio. Elaborado por el autor.*

Configuración de contraseña de usuario

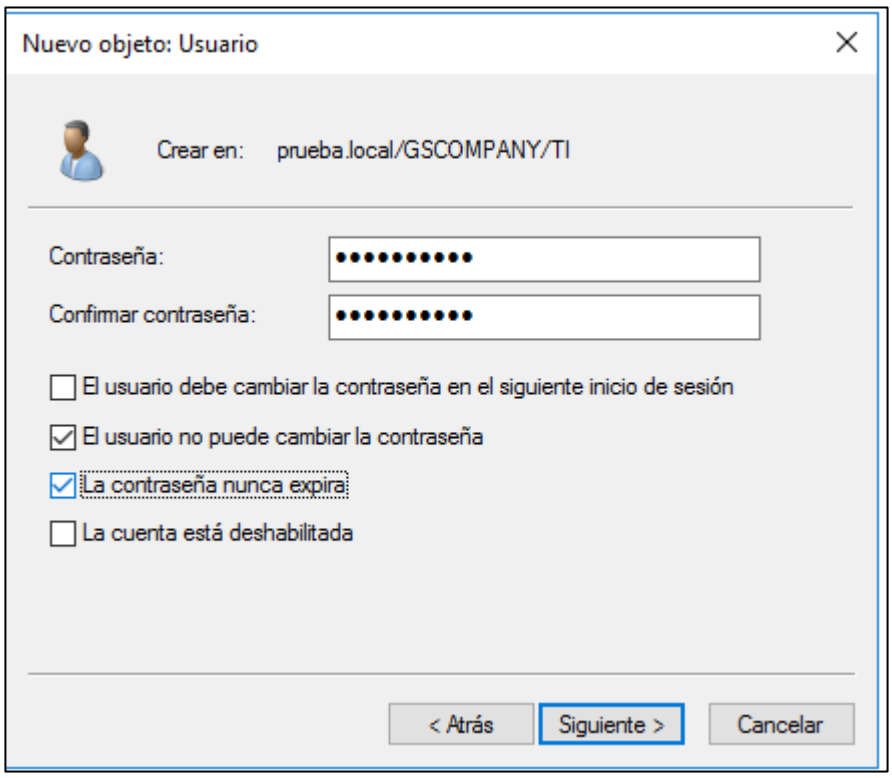


Figura 70. *Configuración de contraseña de usuario. Elaborado por el autor*

Usuarios asignados en la unidad organizativa

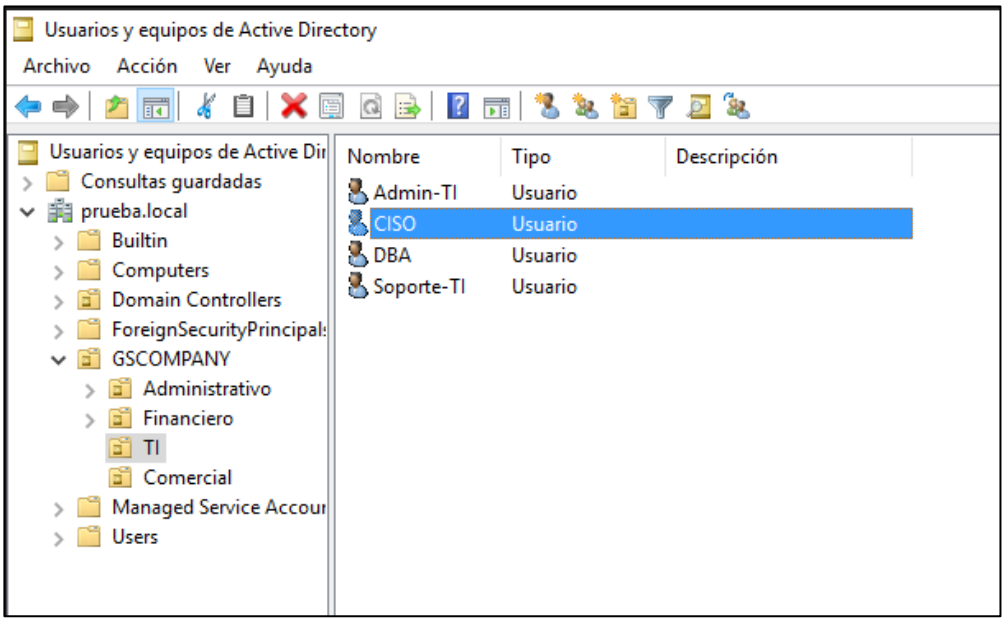


Figura 71*.Usuarios asignados a la Unidad Organizativa. Elaborado por el autor.*

1.4.5 Crear grupos de seguridad

1) Crear un nuevo grupo y asignar privilegios de seguridad

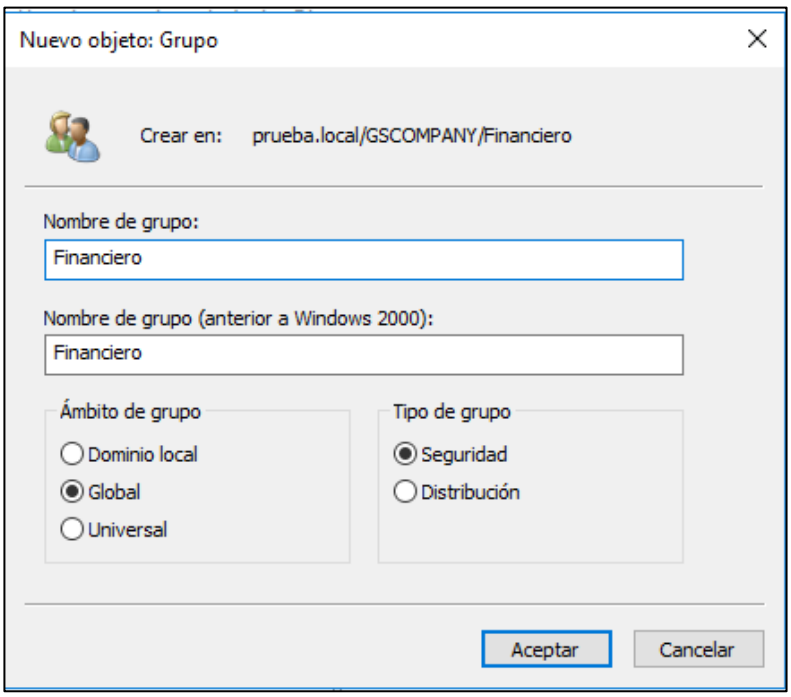


Figura 72. *Creación de cuentas de servicio. Elaborado por el autor.*

2) Agregar el grupo de seguridad al grupo de administradores

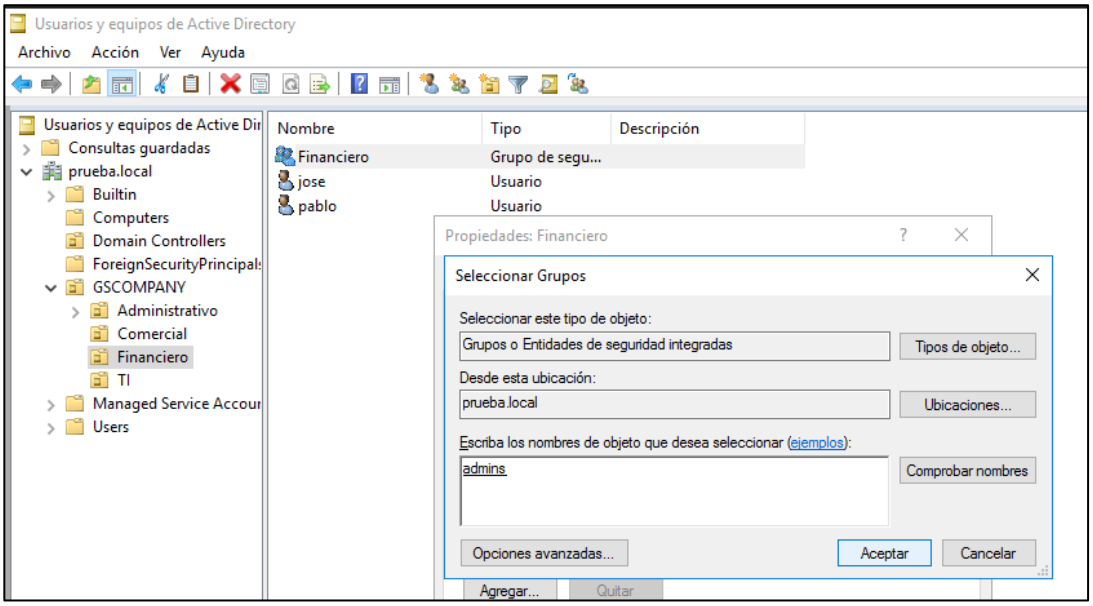


***Figura 73**. Agregar cuenta de servicio al grupo de seguridad. Elaborado por el autor.*

Agregar usuarios al grupo de seguridad

1) Seleccionar las propiedades del usuario.

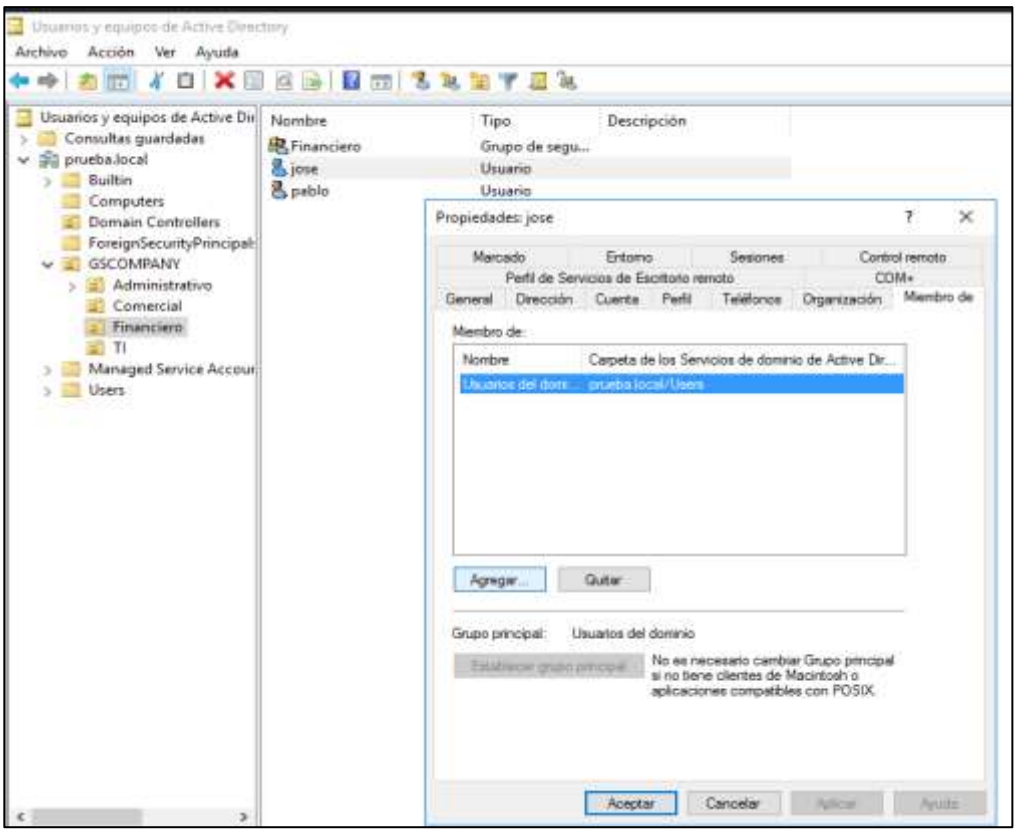


***Figura 74.** Propiedades del usuario. Elaborado por el autor.*

2) Seleccionar el grupo de seguridad donde será agregado el usuario.

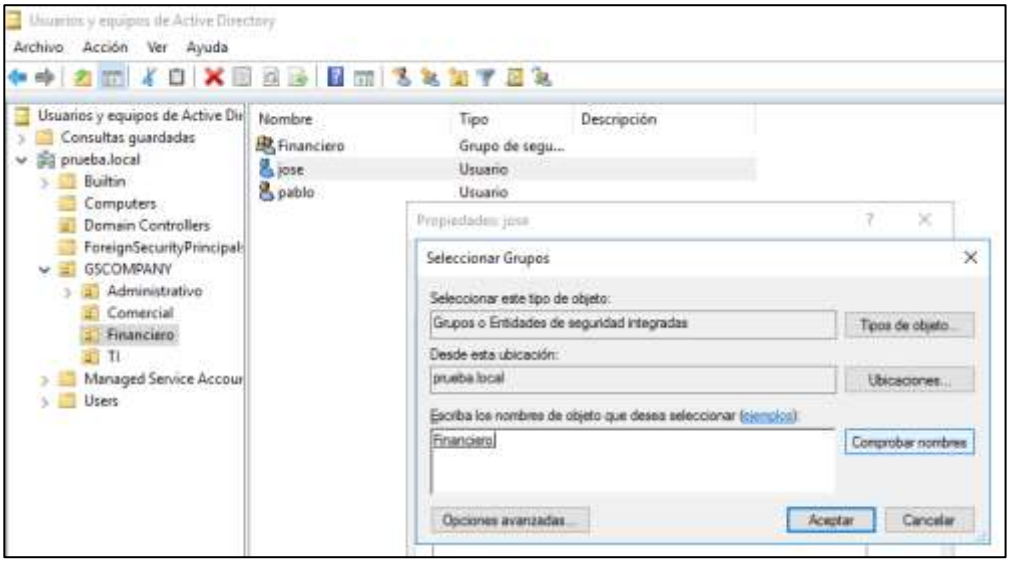


Figura 75. *Selección de grupo de seguridad para usuario. Elaborado por el autor*

1.4.6 Cuentas de servicio

1) Crear un usuario genérico de servicio

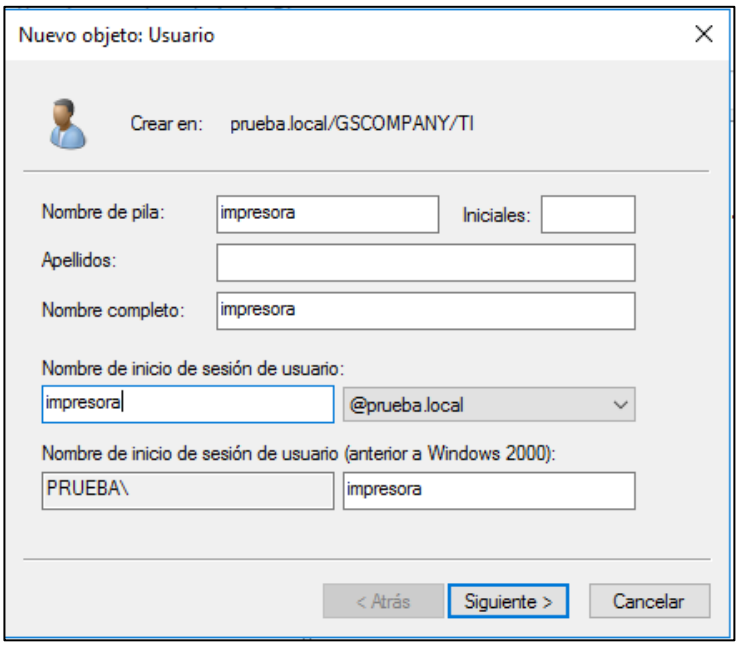


Figura 76. *Creación de cuenta de servicios. Elaborado por el autor*

2) Agregar cuenta de servicio al grupo administradores

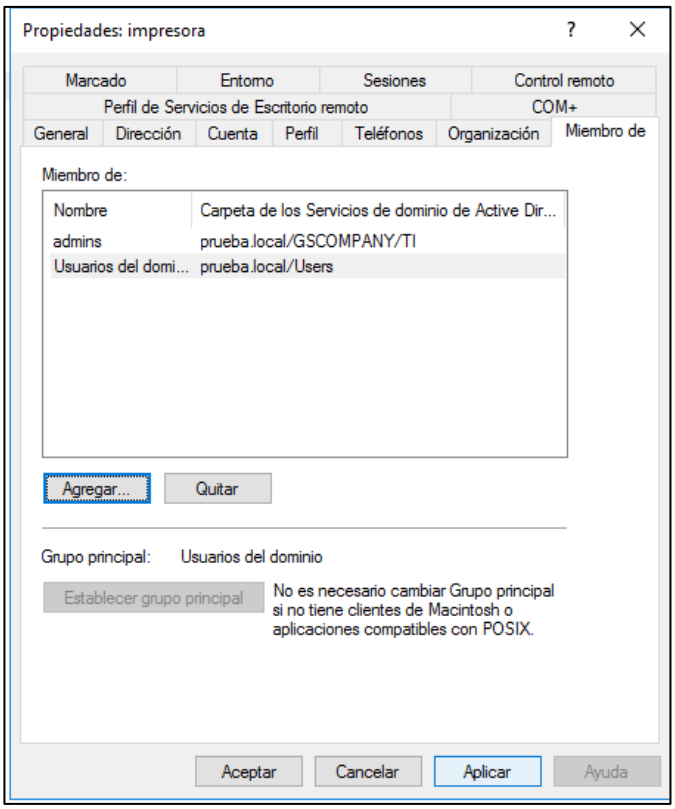


Figura 77. *Unión de cuenta de servicio a grupo de seguridad. Elaborado por el autor*

1.4.7 Políticas de Grupo predeterminadas

Figura 78.*Politicas de Grupo de Active Directory. Elaborado por el autor.*

1.4.5 Agregar equipo cliente al dominio

Configuración DNS en maquina cliente.

1) Configurar dirección IP del servidor como servidor DNS en la maquina cliente

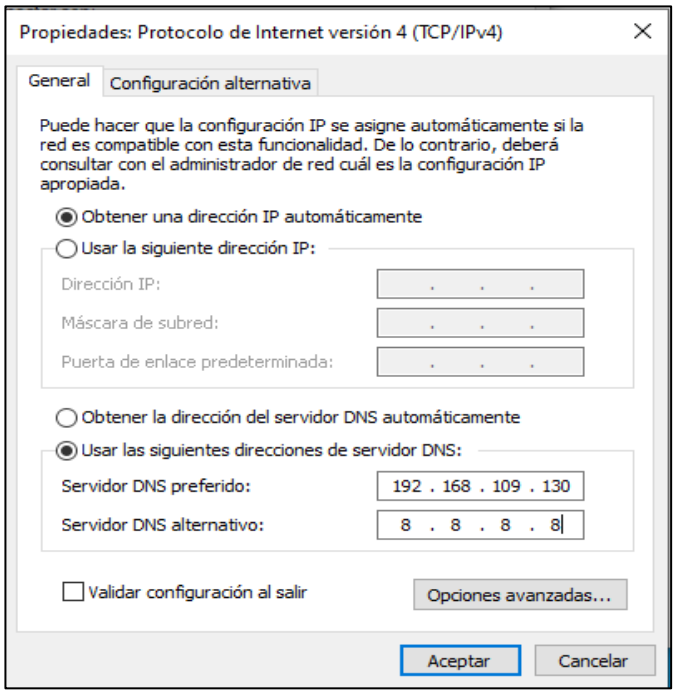


Figura 79*. Configuración DNS en equipo cliente. Elaborado por el autor*

2) Verificación de conexión al servidor haciendo ping al DNS: 192.168.109.130

```
C:\Users\Windows 10>ping 192.168.109.130

Haciendo ping a 192.168.109.130 con 32 bytes de datos:
Respuesta desde 192.168.109.130: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.109.130: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.109.130:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Figura 80. *Ping al servidor DNS. Elaborado por el autor*

3) Utilizar la herramienta de acceso a trabajo o escuela en las configuraciones de sistema de la maquina cliente.

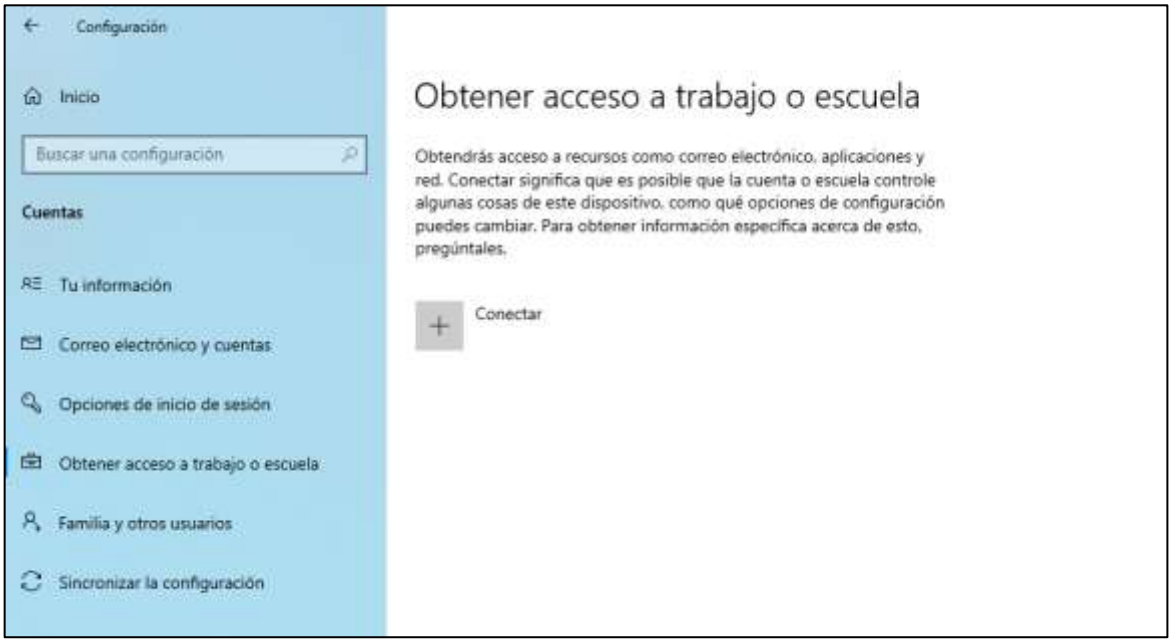


Figura 81. *Acceso a trabajo o escuela. Elaborado por el autor*

4) Utilizar la opción de unirse a un servidor de Active Directory

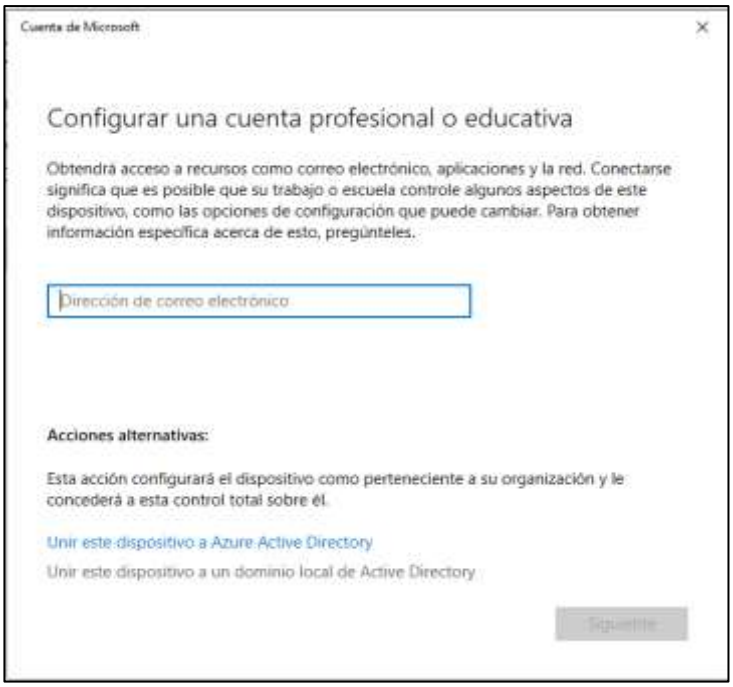


Figura 82. *Unión al servidor de Active Directory. Elaborado por el autor*

5) Agregar el nombre del dominio

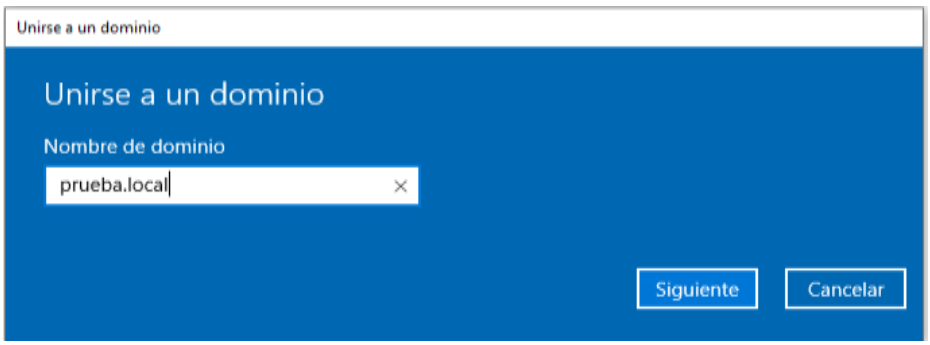


Figura 83. *Unión al dominio. Elaborado por el autor*

6) Agregar la cuenta de usuario y el tipo de cuenta.

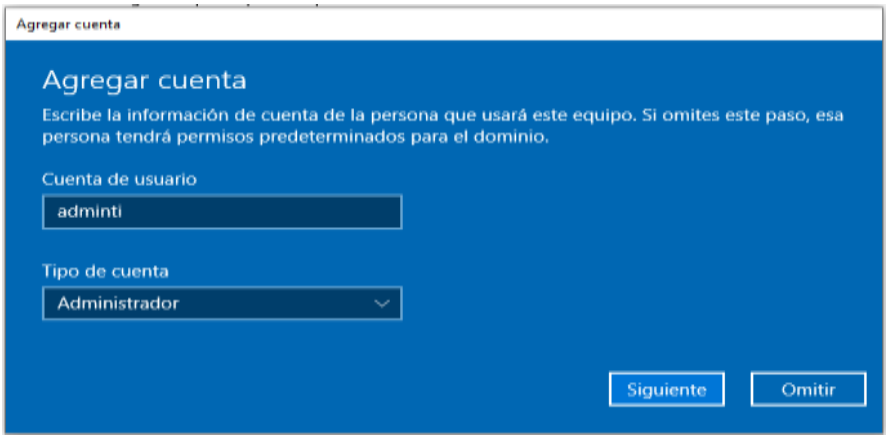


Figura 84. *Ingreso de cuenta de usuario al dominio. Elaborado por el autor*

7) Maquina cliente unida al servidor de dominio

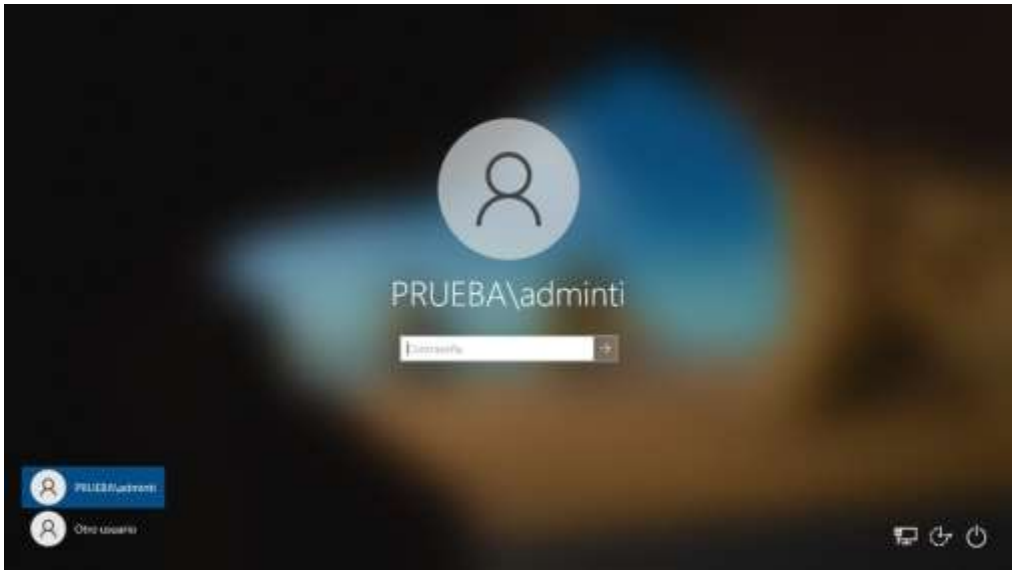


Figura 85. *Maquina cliente unida al dominio. Elaborado por el autor*

2.2 Fase de reconocimiento

2.2.1 Reconocimiento con Net user

Reconocimiento de usuarios de la red con **Net user**

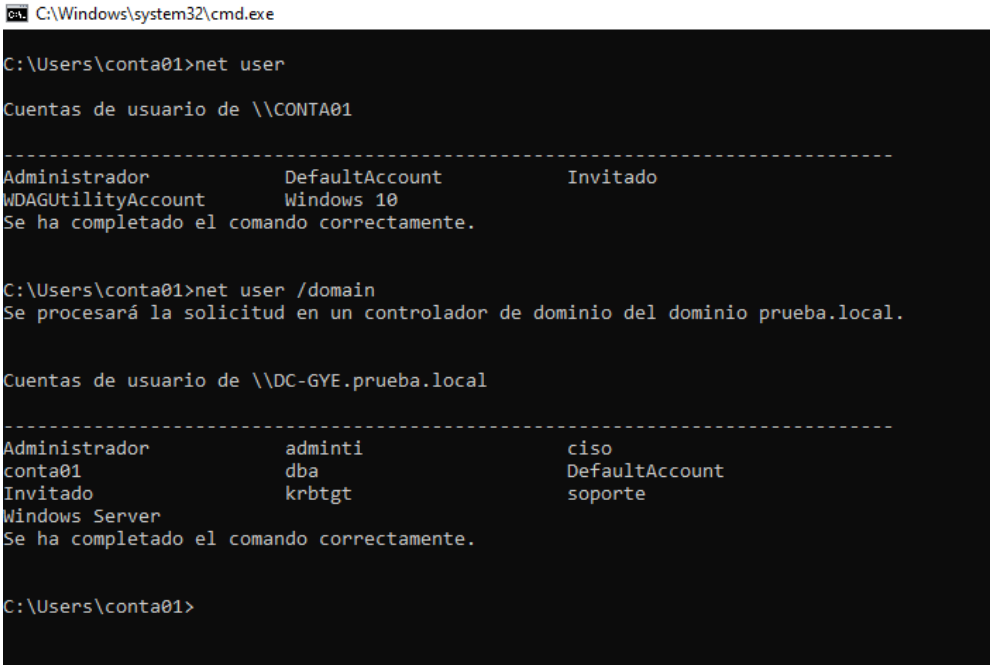


***Figura 86**. Reconocimiento de con Net user. Elaborado por el autor*

Reconocimiento a usuarios del dominio con net user domain <nombre usuario>

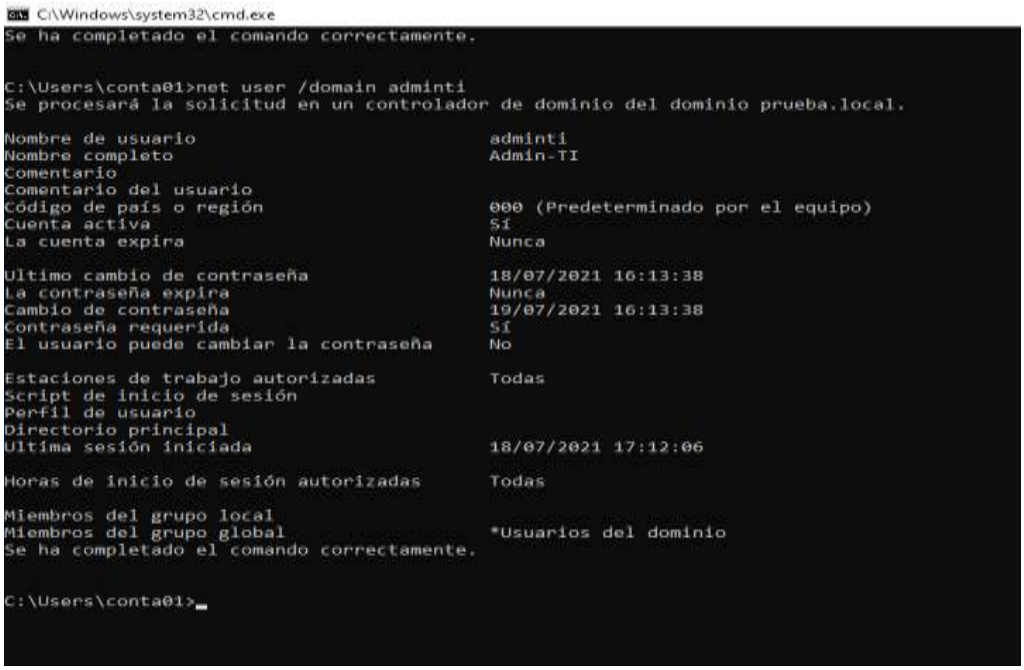


***Figura 87**. Reconocimiento de usuario del dominio. Elaborado por el autor*

2.2.2 Reconocimiento Rsop.msc

Reconocimiento de políticas de grupo (GPO) con **rsop.msc**

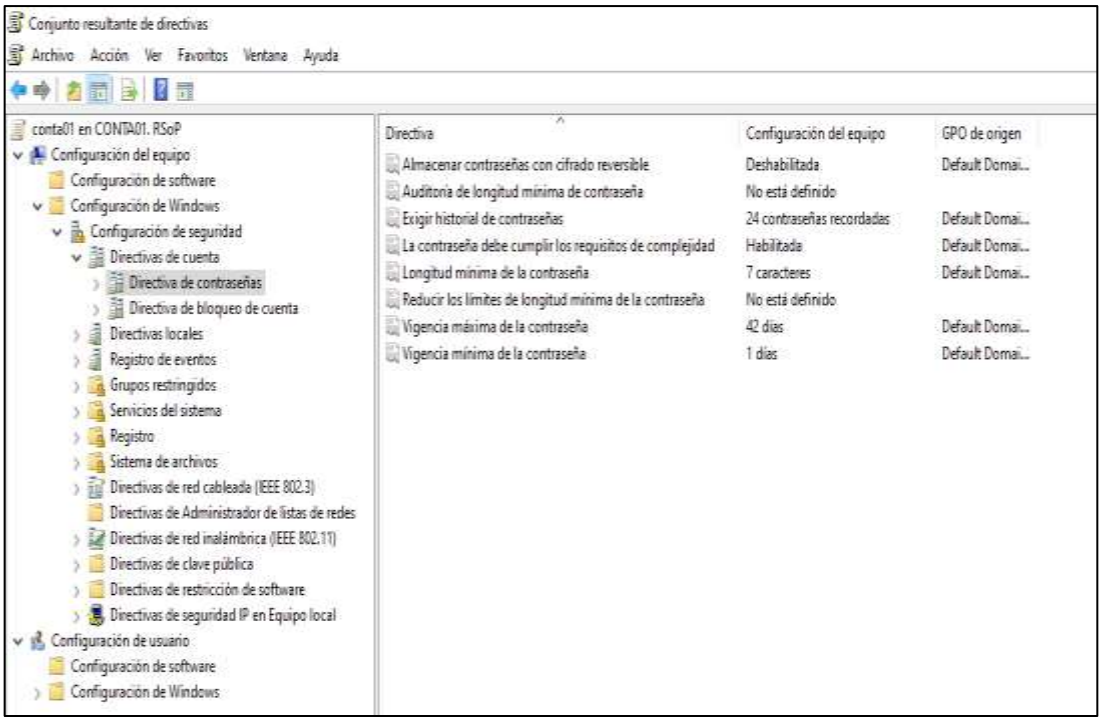


Figura 88. *Reconocimiento con rsop.msc. Elaborado por el autor*

2.2.3 Reconocimiento con GPResult

Reconocimiento de políticas de grupo (GPO) con **gpresult /r**

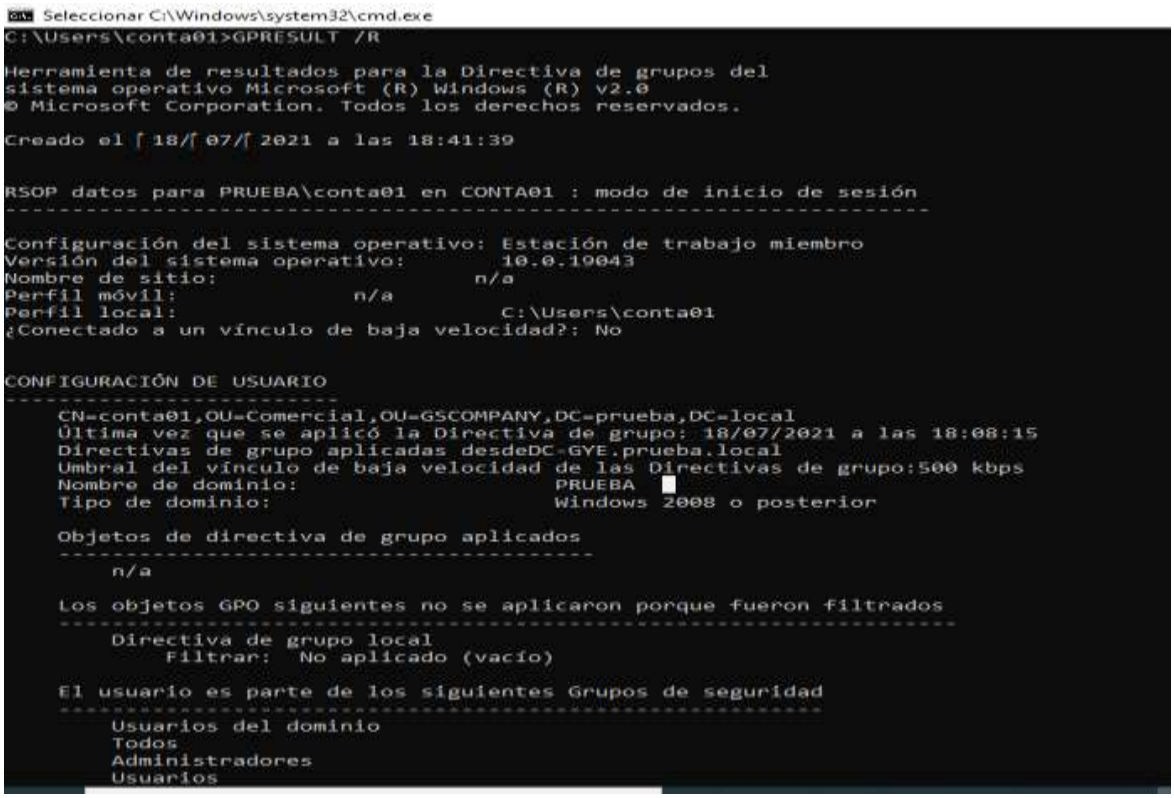


Figura 89. *Reconocimiento con gpresult /r. Elaborado por el autor*

2.3 Fase de escaneo

2.3.1 Escaneo con Nmap

Escaneo de puertos abiertos con nmap < dirección ip>.

Figura 90. *Escaneo de puertos con nmap. Elaborado por el autor*

Escaneo de puertos abiertos, versión y detección de sistema operativo con el comando -O -sV <dirección ip>.

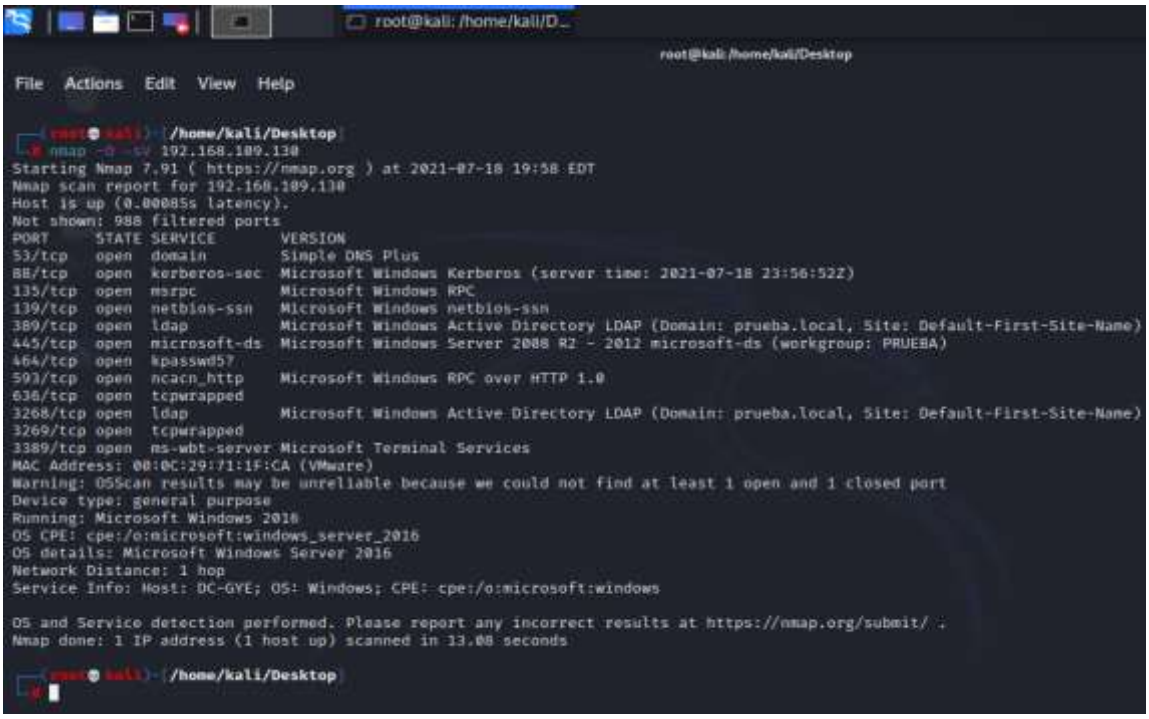


Figura 91.*Escaneo de puertos y versión de Sistema operativo. Elaborado por el autor*

Escaneo de vulnerabilidades en los puertos abiertos con **--script vuln < dirección ip>**

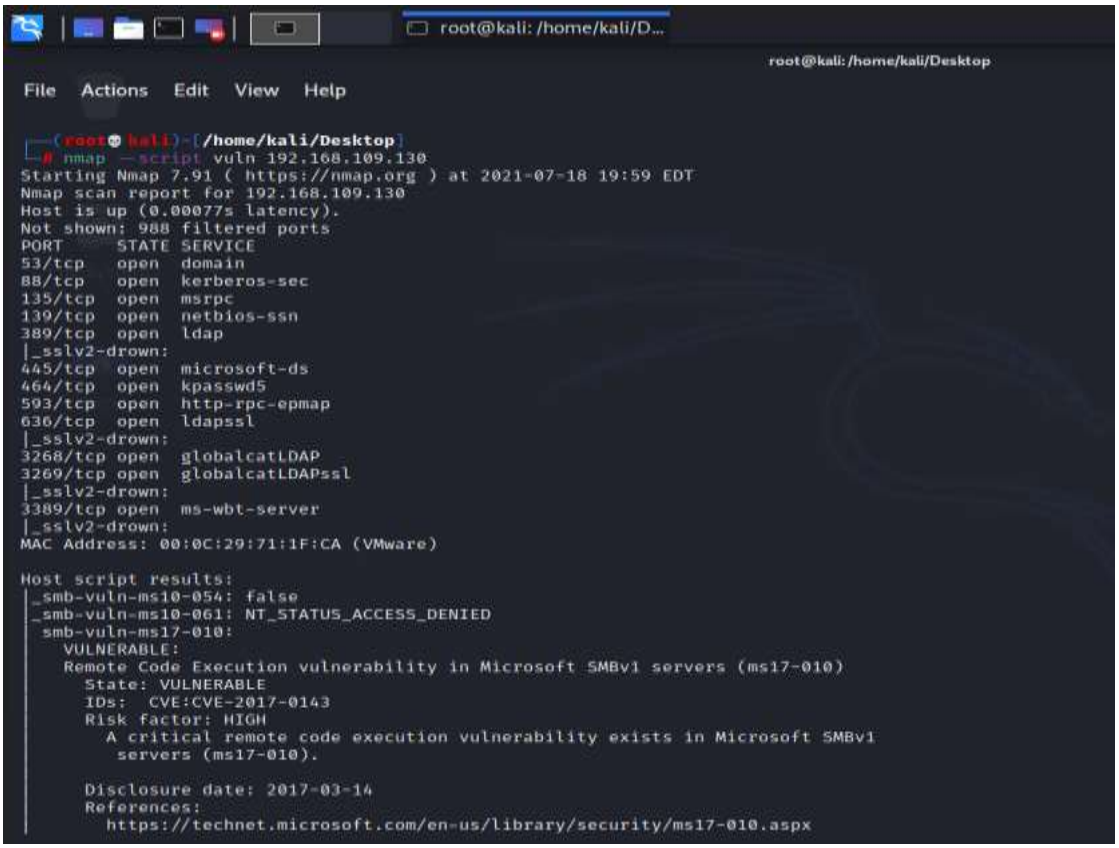


***Figura 92**. Escaneo de vulnerabilidades. Elaborado por el autor*

2.3.2 Escaneo con Nessus

Descarga del paquete Nessus para Kali Linux

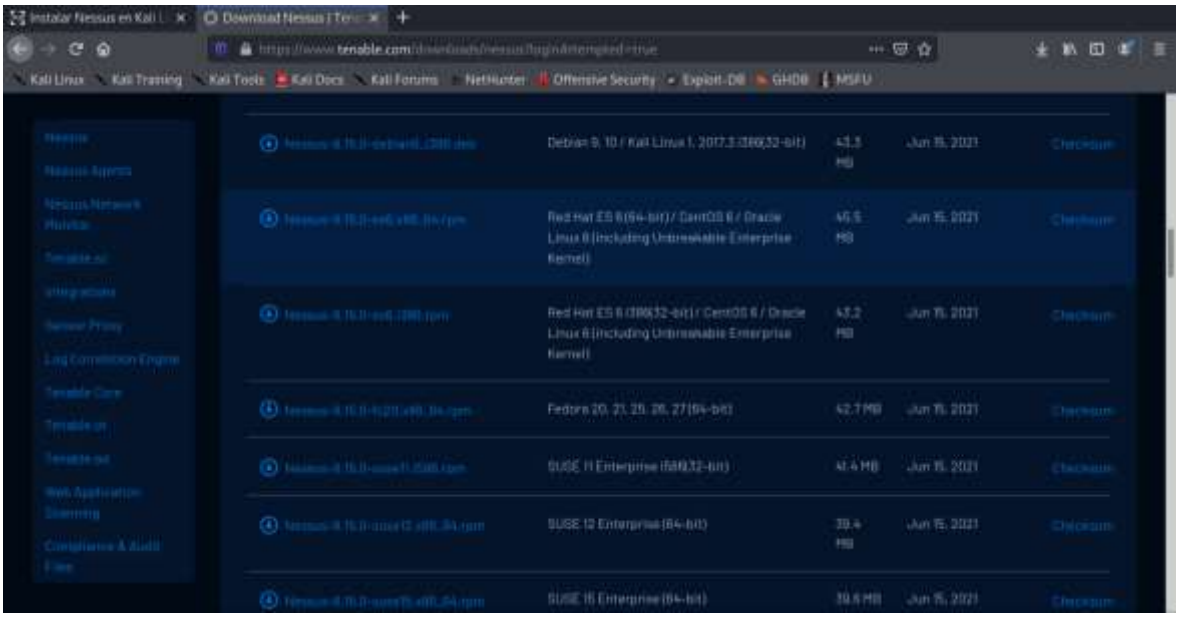


Figura 93. Descarga de Nessus 8.15. Elaborado por el autor

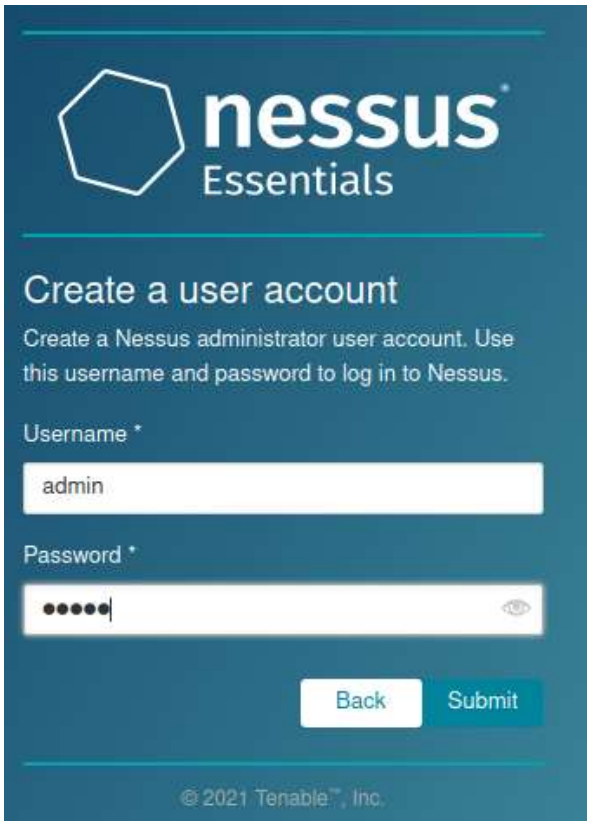


Figura 94. *Creación de cuenta de usuario Nessus. Elaborado por el autor*

Elegir los objetivos de escaneo < direcciones ip>

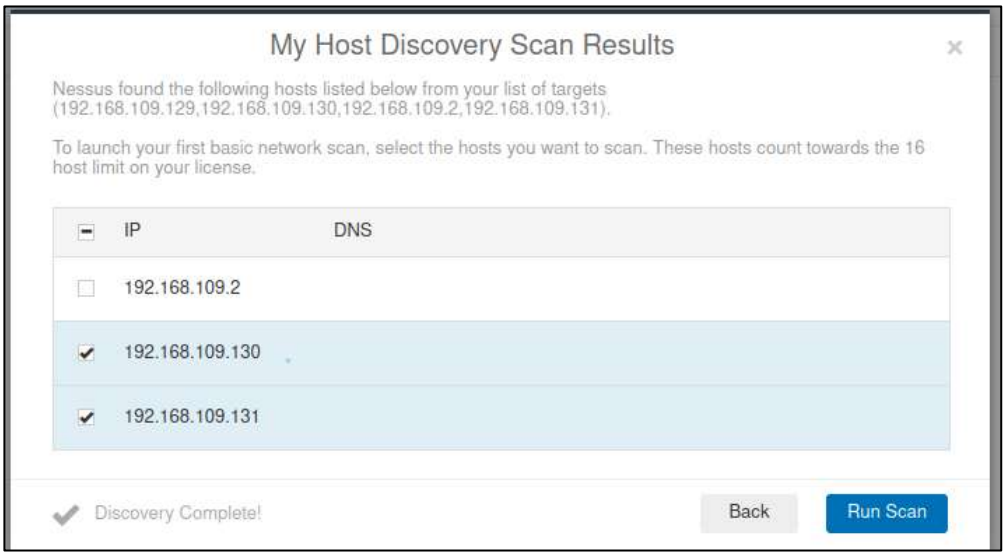


Figura 95. *Elección de objetivos de escaneo. Elaborado por el autor*

Resultados de escaneo de vulnerabilidades con Nessus

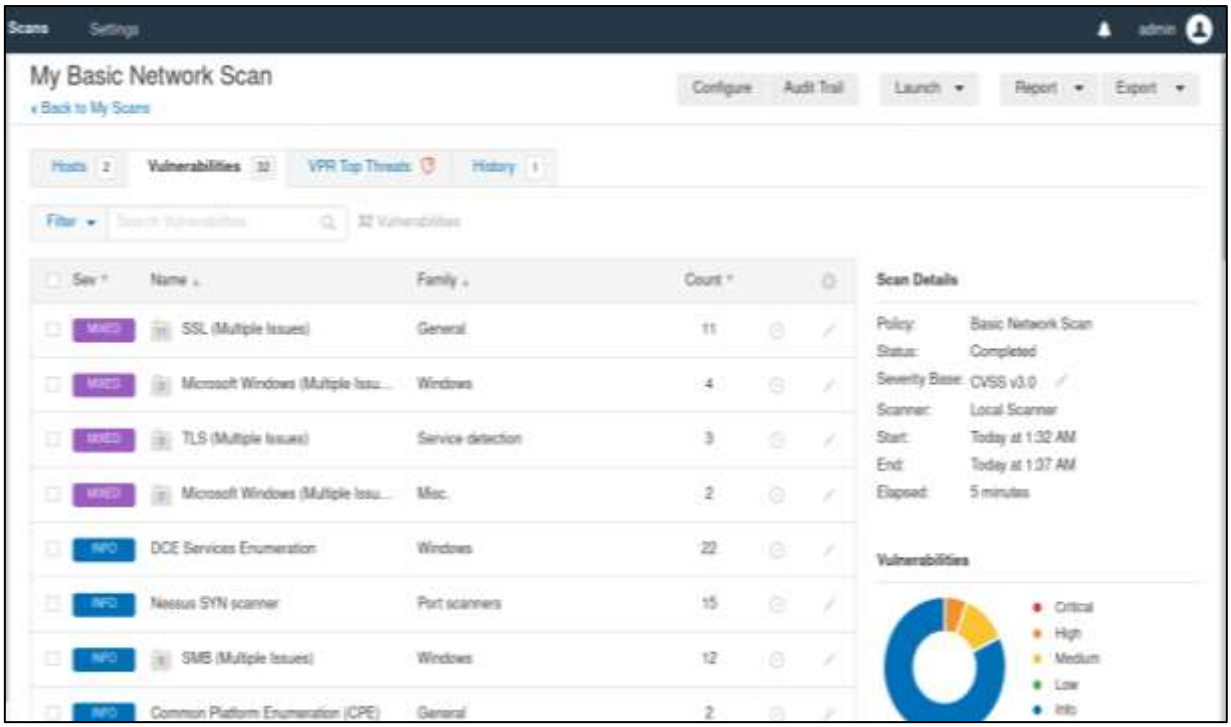


Figura 96*. Resultado de escaneo con Nessus. Elaborado por el autor*

Generar reporte PDF de vulnerabilidades

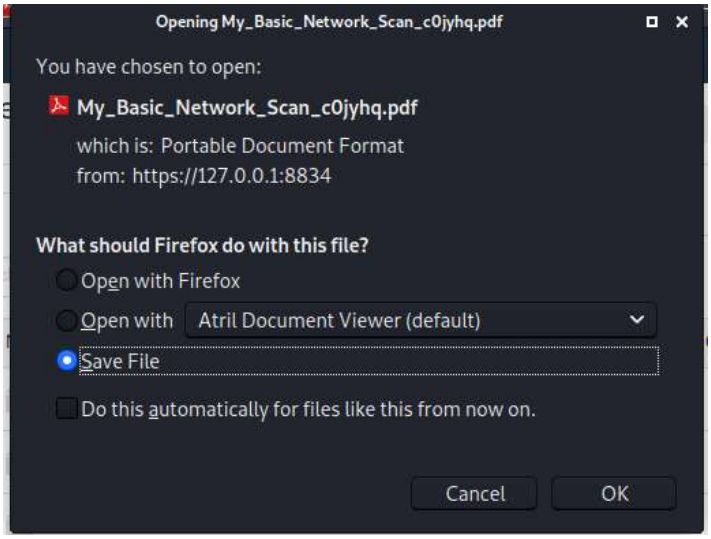
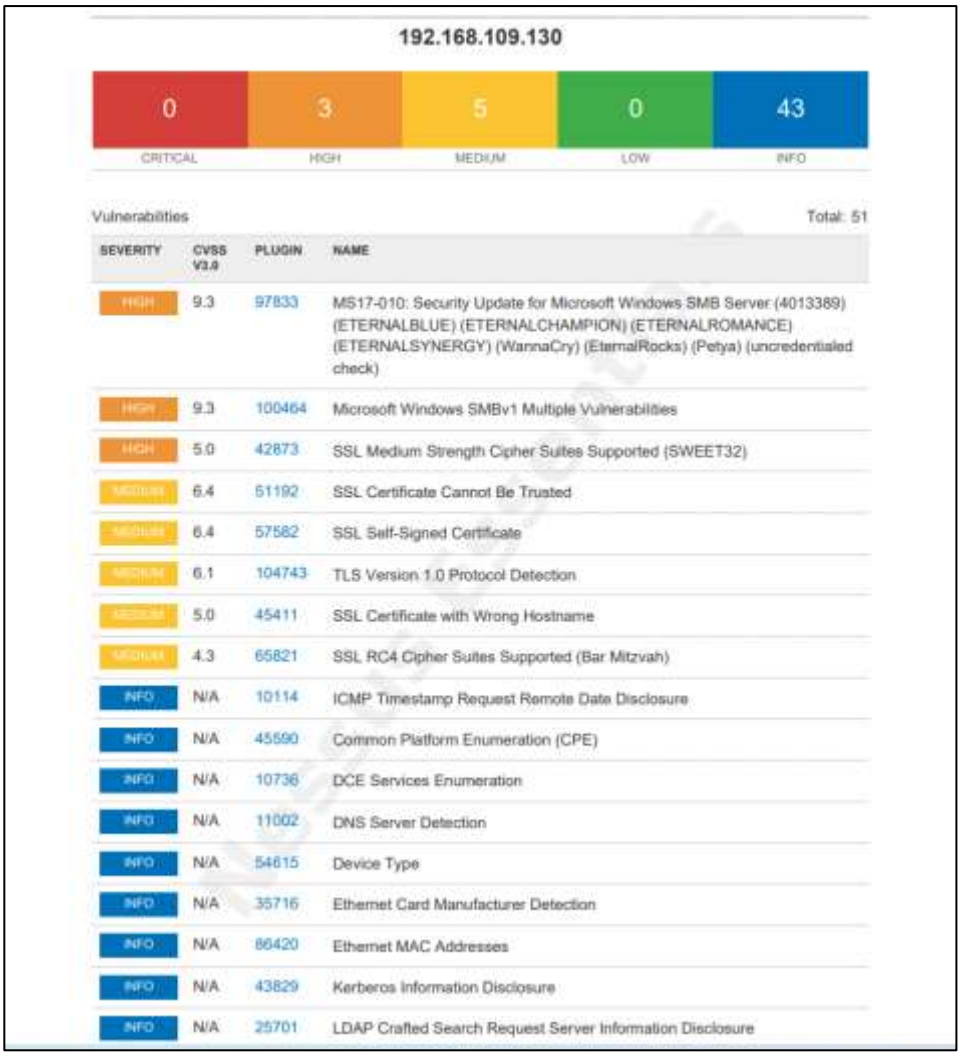


Figura 97.*Reporte PDF de vulnerabilidades. Elaborado por el autor.*



192.168.109.130

0	3	5	0	43
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 51

SEVERITY	CVSS V3.0	PLUGIN	NAME
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	9.3	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure

Figura 98. *Reporte de vulnerabilidades en el servidor de Active Directory. Tomado de reporte PDF de escaneo Nessus. Elaborado por el autor*

2.4 Fase de enumeración

2.4.1 Enumeración con ntbscan

Enumeración de los equipos conectados a la red con **ntbscan -r.**

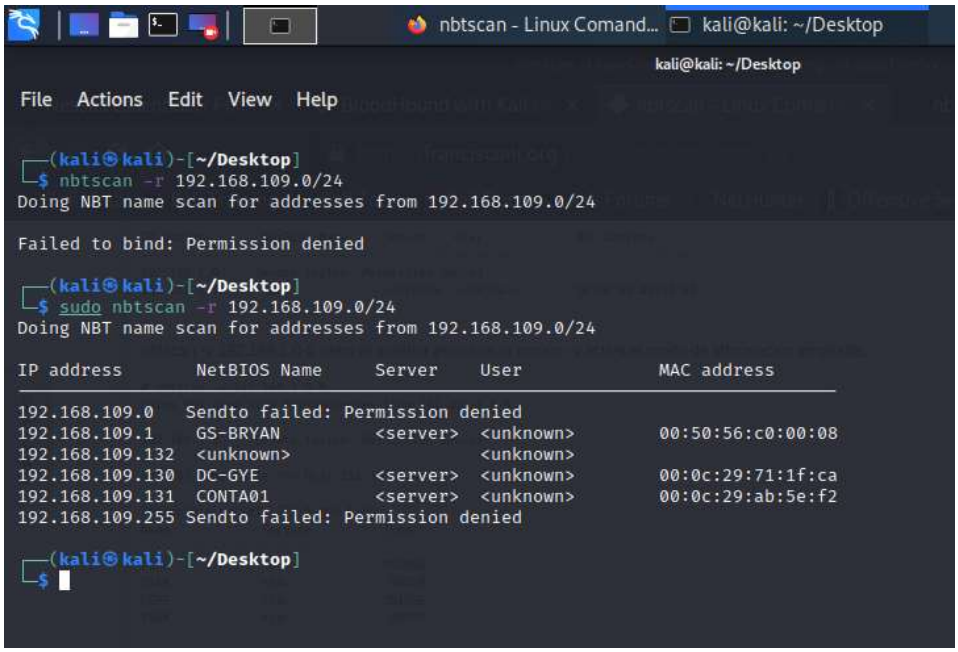


***Figura 99**. Enumeración de equipos en la red. Elaborado por el autor*

2.4.2 Enumeración con enum4linux

Enumeración de la información del dominio y versión de sistema operativo.

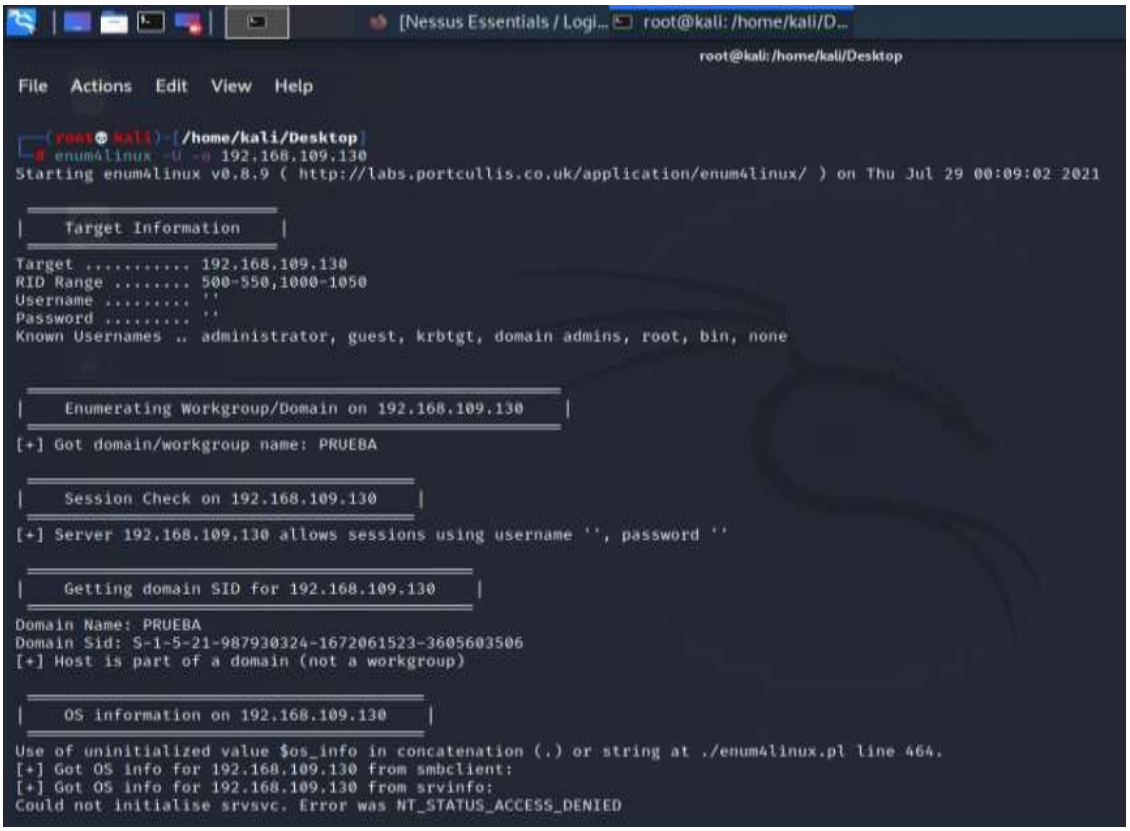


***Figura 100.** Enumeración de información del servidor. Elaborado por el autor*

Bibliografía

Acosta Herran, J. S. (2018). DISEÑO DE UN MODELO DE POLITICAS DE SEGURIDAD PARA UN SERVIDOR. BOGOTÁ: UNIVERSIDAD COOPERATIVA DE COLOMBIA.

Ángel Miguel, G. P. (30 de marzo de 2019). LinkedIn Corporation. Obtenido de LinkedIn: https://www.linkedin.com/pulse/redes-centralizadas-vs-distribuidas-miguel-%C3%A1ngel-p%C3%A9rez-garc%C3%ADa/?originalSubdomain=es

Arias Villafuerte, M. B., & Isabel, H. P. (2015). EACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SIGUIENDO LA NORMA NTE INEN ISO/IEC 27001 – 2013 DE LA FACULTAD A DE CIENCIAS MATEMÁTICAS Y FÍSICAS ESCUELA DE CARRERA DE INGENIERÍA DE SISTEMAS Y NETWORKING DE LA UNIVERSIDAD DE GUAYAQUIL. Guayaquil: Universidad de Guayaquil.

BrandPost. (27 de mayo de 2021). saya comunicaciones s.a.c - idg comunicaciones. Obtenido de cioperu.pe: https://cioperu.pe/articulo/32381/active-directory-5-errores-de-configuracion-que-ponen-en-riesgo-a/

Cristian David, A. F., & Castro, J. A. (2020). VERIFICACIÓN DEL GRADO DE INSEGURIDAD DE LAS INFRAESTRUCTURAS WINDOWS DE DIRECTORIO ACTIVO Y CONSTRUCCION DE UNA GUIA DE ASEGURAMIENTO QUE ELEVE EL NIVEL DE SEGURIDAD ENCONTRADO. BOGOTÁ D.C: UNIVERSIDAD CATÓLICA DE COLOMBIA. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/25758/1/Verificaci%2b%c2%a6n%20del%20grado%20de%20inseguridad%20de%20las%20infraestructuras%20Windows%20de%20DA%20y%20construccion%20de%20una%20guia%20de%20aseguramiento%20que%20eleve%20el%20nivel%20de%2

Daniel, B. (2011). Hacking desde cero. Buenos Aires: Red Users .

DATTA. (21 de enero de 2021). DATTA. Obtenido de datta.com.ec: https://datta.com.ec/articulo/ecuador-una-de-las-naciones-mas-atacadas-por-los-hackers#:~:text=Seg%C3%BAn%20la%20empresa%20de%20seguridad,de%20software%20malicioso%20o%20malware.&text=En%20el%202019%2C%20en%20Am%C3%A9rica,pa%C3%ADses%20como%20M%C3%A9xico%

Deloitte. (2018). Informe de Encuesta 2018 sobre Tendencias de Cyber Riesgos y Seguridad de la Información en Ecuador. Guayaquil: Deloitte.

Deloitte. (2020). Estado actual de la ciberseguridad 2020. Guayaquil: Deloitte.

Domínguez Sanjuán, M. (2018). Virtualización mediante entornos Open Source. Valencia: Universidad Politecnica de Valencia.

ESET. (2020). ESET Security Report Latinoamérica 2020. ESET.

Felix Xavier, Q. A., & Javier Ernesto, S. C. (2018). ANÁLISIS DE VULNERABILIDADES EN LOS SERVICIOS ACTIVE DIRECTORY, DNS Y DHCP INSTALADOS EN LOS SISTEMAS OPERATIVOS WINDOWS SERVER (2008, 2012, 2016) UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN. Guayaquil: Universidad De Guayaquil.

Fernández Bermejo, D., & Martínez Atienza, G. (2018). Ciberseguridad, Ciberespacio y Ciberdelincuencia.

Folgueiras Bertomeu, P. (2016). Técnica de recogida de información: La entrevista. Catanlunya : Universitat de Barcelona .

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de.

GOMEZ, M. A. (2010). "DISEÑO E IMPLEMENTACIÓN DEL SERVICIO DE DIRECTORIO ACTIVO EN LA RED DE LA GOBERNACIÓN Y ESQUEMATIZACIÓN DEL DIRECCIONAMIENTO IP EN LA RED DE DATOS DEPARTAMENTAL". repositorio.ucp.edu.co.

Guevara Alban, G. P., Verdesoto Arguello, A. E., & Castro Molina, N. E. (julio de 2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). ReciMundo, 4(3), 163-173. doi:10.26820/recimundo/4.(3).julio.2020.163-173Reconocimiento-NoComercial-CompartirIgualCC BY-NC-SAEsta licencia permite a otros entremezclar, ajustar y construir a partir de su obra con fines no comerciales, siempre y cuando le reconozcan la autoría y sus nu

Huertas Alonso, Y. A., & Tapias Alban, H. F. (2016). DISEÑO E IMPLEMENTACIÓN DE UNA METODOLOGÍA DE HARDENING PARA LOS SERVIDORES, ESTACIONES DE TRABAJO Y DIRECTORIO ACTIVO DEL MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO. Bogotá: UNIVERSIDAD PILOTO DE COLOMBIA.

Ignacio Martín, G. U. (2018). Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada. La Plata: Universidad Nacional de la Plata.

INCIBE. (16 de septiembre de 2020). INCIBE (Insitituto Nacional de de Ciberseguridad). Obtenido de Incibe.es: https://www.incibe.es/protege-tu-empresa/avisos-seguridad/vulnerabilidad-critica-del-protocolo-netlogon-las-versiones

Jean-François. (2017). Windows Server 2016 - Arquitectura y Administración de los servicios de dominio Active Directory (AD DS). Ediciones Eni.

Jesus Macario, G. G. (30 de mayo de 2015). slideshare. Obtenido de es.slideshare.net: https://es.slideshare.net/JesusGarciaGuevara/protocolos-usados-por-ad-ds

Jorge Enrique, A. C. (mayo de 2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. Revista Científica Aristas, 2(1), 18-27. Obtenido de https://revistacientificaistjba.edu.ec/images/home/documentos/Mayo_2020/2.pdf

José Daniel, F. F. (2020). Gestión ágil de usuarios en dominios Active Directory mediante un portal web. Valencia: Universidad Politecnicade Valencia.

Julian Hernan, B. C. (2018). DISEÑO DE MANUAL DE DIAGNOSTICO Y PREVENCION DE VULNERABILIDADES EN REDES DE DATOS PARA PYMES. Bogotá: UNAD Colombia.

LEÓN, A. D. (22 de mayo de 2019). hostingdiario. Obtenido de https://hostingdiario.com/windows-server/#Caracteristicas_de_Microsoft_Windows_Server

López de Jiménez, R. E. (Diciembre de 2017). PRUEBAS DE PENETRACIÓN EN APLICACIONES WEB USANDO HACKEO ÉTICO. REVISTA TECNOLÓGICA(10), 13-19.

Maité Martínez González, Y. H. (2018). SISTEMA PARA LA GESTIÓN DE USUARIOS DEL DIRECTORIO ACTIVO.

Manageengine. (20 de Abril de 2019). Zoho Corporation. Obtenido de Manageengine.com: https://www.manageengine.com/latam/ad-manager/cinco-errores-administracion-de-active-directory.html

Microsoft. (8 de mayo de 2018). docs.Microsoft.com. Obtenido de Microsoft 2021: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/executive-summary

NCSI. (14 de Agosto de 2019). NCSI. Obtenido de ncsi.ega.ee: https://ncsi.ega.ee/country/ec/

Ortiz, A. E. (27 de julio de 2018). HostDime Argentina. Obtenido de www.hostdime.com.ar: https://www.hostdime.com.ar/blog/que-es-una-maquina-virtual-definicion-vm/

Pastor Ricós, F. (2020). Pentesting y generación de exploits con Metasploit.

Ramirez Cuesta, Y. (27 de agosto de 2014). IT NOW . Obtenido de revistaitnow.com: https://revistaitnow.com/como-evitar-nueve-errores-comunes-de-active-directory/

Reyes Romero, C., Mejía Sáenz, K., & Sánchez Carlessi, H. H. (2018). Manual de términos en investigación científica, tecnológica y humanística. Lima: Universidad Ricardo Palma.

Robaypo López, J. H., & Rodríguez Rodríguez, R. M. (2015,). Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net. Bogotá: UNAD.

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Adriana, M. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.

Sain, G. (2018). ¿Qué es la seguridad informáTICA?

Salamanca, O. (Diciembre de 2016). Sistema de gestión de seguridad para redes de área local para empresas desarrolladoras de software. Revista Venezolana de Información, Tecnología y Conocimiento, 13(3), 114-130.

Tamayo Argoti, L. D. (2020). Tecnicas de Ingenieria Social aplicadas a estudiantes de grado 11° de la ciudad de San Juan de Pasto.

Toapanta, R. H. (2015). “IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA RED LAN CON TECNOLOGÍA IPV4 BAJO LA PLATAFORMA WINDOWS PARA PROVEER SERVICIOS EN EL LABORATORIO DE REDES Y MANTENIMIENTO EN LA UNIVERSIDAD TÉCNICA DE COTOPAXI EXTENSIÓN LA MANÁ”. La Maná: http://repositorio.utc.edu.ec.

Torres Núñez, E. M. (2015). “Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato”. Ambato: Universidad Tecnica de Ambato.

Vázquez, J. C. (30 de marzo de 2021). CIO Mexico. Obtenido de 2021 Ediworld SA de CV: https://cio.com.mx/directorio-activo-el-recurso-que-la-empresa-no-debe-perder-de-vista/