Hardenización: Proceso Escencial para la Seguridad Informática

Luis Felipe López Ruíz
flopezr@gmail.com
Universidad Piloto de Colombia

Resumen - A raíz de la pandemia generada por el COVID-19 las empresas vieron la necesidad de implementar nuevos modelos tecnológicos o modificar los existentes a fin de poder afrontar las nuevas modalidades de trabajo generadas por este suceso, en el afán de poder continuar en sus actividades se implementaron productos que permitieran de una forma rápida seguir operando generando una dependencia tecnológica aun mayor, esto hace que el área de ciberseguridad o los responsables de la misma, estén revisando cada día los controles necesarios para garantizar el cumplimiento de los pilares de la seguridad de la información, confidencialidad, integridad y disponibilidad para lo cual se hace necesario la revisión en sus infraestructura tecnológicas de los controles necesarios que garanticen el adecuado aseguramiento de la misma.

Índice de Términos— Sistema Operativos, Hardening, Herramientas, Seguridad de la información, Ciberseguridad.

Abstract - As a result of the pandemic due to COVID-19, companies saw the need to implement new technological models or modify existing ones in order to be able to face the new work modalities generated by this event. in an effort to continue their activities, companies implemented products that quickly allowed them to continue operating, causing an even greater technological dependency, this means that the cybersecurity area or those responsible for it are reviewing the necessary controls every day to guarantee compliance with the security pillars of the information, confidentiality, integrity and availability for which it is necessary to review the necessary controls in its technological infrastructure to guarantee its adequate assurance.

I. INTRODUCCIÓN

La ciberseguridad se ha convertido en uno de los temas más relevantes en las empresas sin importar su tamaño o actividad económica, teniendo en cuenta que cada vez la dependencia a nivel tecnológica para el acceso y procesamiento de la información es mayor se hace necesario contar con técnicas que permitan lograr el aseguramiento de la misma implementando controles que permitan lograr este objetivo. Aplicar ciberseguridad en los ecosistemas tecnológicos no es fácil, se necesita contar con personal calificado, lleva tiempo e inversión, se vuelve un reto organizacional, sin embargo, implementar ciberseguridad es una práctica escalonada que puede ser ejecutada por niveles. En este articulo ampliaríamos sobre un primer nivel de aseguramiento conocido como hardening o endurecimiento de los sistemas haciendo énfasis en sistemas operativos Microsoft.

II. HARDENING

El hardening es una técnica de ciberdefensa que busca evitar la interrupción en los sistemas informáticos por un ciberataque el cual pueda comprometer la integridad, disponibilidad y confidencialidad de la información. [1]

El proceso de hardening implica tomar acciones proactivas que permitan minimizar la cantidad de formas en la que un atacante pueda obtener acceso no autorizado a un dispositivo, una red o un sistema de información, por medio de configuraciones cuyo objetivo es fortalecer los sistemas para que sean lo más seguro posibles.

Entre estas acciones se encuentran:

- Actualizaciones de Software, que permiten mantener el system y el software actualizado con las últimas correciones y parches de seguridad disponibles, configuraciones Seguras de sistemas y aplicaciones deshabilitando o limitando caracteristicas y servicios no necesarios o potencialmente inseguros.

- Uso de Firewall, por medio del cual se controle el tráico de red y permita el bloqueo de accesos no autorizados.

- Gestión de cuentas y accesos, donde por medio de políticas se establescan contraseñas fuertes y el uso de doble factor de autenticación cuando sea possible.

- Control de privilegios, donde se restrinjan los accesos a los recursos y servicios de los sistemas solo a los usuarios que realmente los necesiten.

- Monitoreo y logs, que permitan identificar acividades inusuales o sospechosas

- Encriptación, que proteja la confidencialidad de los datos en reposo o tránsito.

- Concienciación, donde los usuarios aprendan sobre las buenas practicas de seguridad y cómo identificar posibles amenazas a las cuales pueden ser expuestos, como el phising o el malware.

El hardening es una tarea fundamental por dos razones principales:

Seguridad: Los delitos informáticos van evolucionando utilizando técnicas de ataque más sofisticadas, sin embargo, se ha demostrado que implementar controles básicos como el hardening generan un mayor impacto en la seguridad de la organización.[1]

Cumplimiento : El hardening es ahora un requisito básico en la mayoría de las normas de seguridad de la información. Regulaciones como PCI-DSS, ISO27001 entre otras, requieren que las organizaciones implementen una sólida política de hardening.[1]

III. ETAPAS PRICIPALES EN UN PROYECTO DE HARDENING

Las tres etapas principales para un proyecto de hardening son:

A. Establecer las políticas de hardening.

Estas políticas deben detallarse tanto como sea posible, se deben tener en cuenta los diferentes entornos, tipos de máquinas, roles y versiones, estas políticas toman como referencia las mejores prácticas de la industria y deben ser ajustadas a las necesidades de la empresa.

B. Realizar un análisis de impacto de las políticas e implementarlas

Se debe analizar el impacto de las políticas para evitar interrupciones en los servicios productivos como resultado de la implementación de las mismas. Es una etapa importante, ya que es propensa a errores que pueden llevar a resultados devastadores. Para minimizar estos impactos, se deben probar en entornos controlados o virtualizados a fin de mitigar el impacto al momento de su aplicación en los entornos productivos.

C. Monitoreo y cumplimiento

El proceso de hardening a menudo se toma como un tarea de una sola vez, sin embargo debido al carácter dinámico de la infraestructura se debe realizar esta actividad de forma periódica, actualizaciones de sistemas, configuraciones aplicadas y nuevas vulnerabilidades hacen que volvamos a un punto inicial antes de aplicar hardening generando riesgos que debemos controlar.

IV. TIPOS DE HARDENING

Aunque un proceso de Hardening es aplicable a toda la infraestructura de una empresa, se debe tener en cuenta que existen varios modelos de endurecimiento que requieren diferentes enfoques y herramientas.[2]

A. Hardening de la red

Los dispositivos de red están configurados para contrarrestar el acceso no autorizado a la infraestructura de una red. En este tipo de endurecimiento, se buscan y corrigen las vulnerabilidades en la gestión y configuración de los dispositivos para evitar su explotación por parte de agentes maliciosos que deseen acceder a la red. Cada vez son mas utilizadas las debilidades en las configuraciones de los dispositivos de red y los protocolos de enrutamiento para establecer una presencia persistente en una red en lugar de atacar endpoints específicos.

B. Hardening de Servidor

El proceso de endurecimiento del servidor gira entorno a la seguridad de los datos, puertos, componentes, las funciones y los permisos de un servidor. Estos protocolos se ejecutan en todo el sistema de hardware, firmware y software.

C. Hardening de la aplicación

El endurecimiento de las aplicaciones se centra en el software instalado en la red, es llamado endurecimiento de software o endurecimiento de aplicaciones de software, se busca aplicar parches y actualizaciones que remedien vulnerabilidades.

Este tipo de endurecimiento puede implicar la actualización o reescritura del código de la aplicación para mejorar su seguridad, o el despliegue de soluciones de seguridad adiciónales basadas en software.

D. Hardening de base de datos

El endurecimiento de las bases de datos se centra en reducir las vulnerabilidades de las bases de datos (Motores) y los sistemas de gestión de bases de datos (SGBD). El objetivo es reforzar los depósitos de datos, así como el software utilizado para interactuar con esos datos.

E. Hardening del sistema operativo

El endurecimiento del sistema operativo implica asegurar un objetivo común de los ciberataques: el sistema operativo de un servidor. Al igual que con otros tipos de software, el endurecimiento de un sistema operativo suele implicar la gestión de parches que puede supervisar e instalar actualizaciones, y paquetes de servicio de forma automática.

F. Hardening de los usuarios

El hardening no solo tiene que ver con software o hardware, también se debe tener en cuenta a los usuarios, este endurecimiento es conocido como concienciación de los usuarios, unos usuarios bien concienciados acerca de los posibles problemas reales son menos propensos a ser vulnerables y, por ende, a que lo sean los sistemas de la empresa. Es importante concientizar a los usuarios en buenas prácticas sobre seguridad informática como:

- No abrir archivos desconocidos
- No descargar archivos de páginas no oficiales
- Tener contraseñas robustas
- Tener precaución con los correos electrónicos
- Tener precaución con mensajes sospechosos de rifas o bloqueos

Un usuario con conceptos claros como los expuestos reducirá el riesgo y aumentará la seguridad informática de la empresa [3].

V. RIESGOS DE NO REALIZAR HARDENING

El no contar con procesos de hardenización actualizados pueden llevar generar riesgos significativos que afecten la seguridad, integridad y confidencialidad de los sistemas y datos. Entre los principales riesgos de no contar con sistemas hardenizados estan:

Ataques de Malware. Los sistemas son mas suceptibles a ser infectados con malware, virus informáticos, rasonware, troyanos y otros tipos de software malicioso los cuales pueden causar daños graves al sistema, robar información confidencial y bloquear el acceso a los datos por medio de ataques de tipo rasomware.

Vulnerabilidades Explotables. Los sistemas pueden tener configuraciones predeterminadas inseguras o servicios innecesarios habilitados, lo que puede facilitar el acceso no autorizado y explotacion de vulnerabilidades por parte de los ciberdelincuentes.

Acceso no Autorizado: Lo cual puede permitir que actores maliciosos obtengan acceso no autorizado a la infraestructura y a los datos sensibles, lo que podria resultar en robo de información, fuga de datos o sabotaje.

Denegación de Servicio (DoS): Los sistemas son mas suceptibles a ataques de denegación de servicios, donde los atacantes saturan el sistema con tráfico malicioso o solicitudes para hacer que se vuelvan inaccesibles para los usuarios legítimos.

Espionaje y Fuga de Información . Los sistemas pueden ser victimas de espionaje cibernético, donde los atacantes obtienen acceso a información confidencial o propietaria y la divulgan a terceros o la utilizan para su propio beneficio.

Interrupción del Negocio : Un ataque exitoso debido a la falta de hardenización puede llevar a la interrupción de las operaciones comerciales, lo que puede resultar en pérdida de productividad y daño a la reputación de la empresa.

Incumplimiento normativo : La falta de hardenización puede llevar al incumplimiento de regulaciones y especificaciones de seguridad de datos lo cual genera incumplimientos exponiendo a las organizaciones a sanciones y multas.

VI. LINEAMIENTOS PARA REALIZAR HARDENING

Al realizar un proceso de Hardening se hace necesario contar con líneas base aceptadas por el mercado como punto de inicio para la actividad a realizar. Existen varias de estas que son una excelente guía para este tipo de ejercicios.

A. DISA – Agencia de sistemas de información de defensa de Estados Unidos

Fig. 1 Logo Agencia de sistemas de información de Defensa de Estados Unidos

Las guías de implementación y técnicas de seguridad (SGTI) de la Agencia de Sistemas de Información de Defensa (DISA) son un conjunto de reglas de mejores prácticas para instalar y respaldar sistemas de TI. Cada STIG se relaciona con un activo específico, por ejemplo, un sistema operativo, una aplicación o una pieza de hardware de la red, y establece las prácticas de configuración y mantenimiento necesarias para garantizar que el activo se configure y administre de manera segura. [4]

Las guías de implementación se encuentran disponibles en la página oficial de DISA donde se puede seleccionar por categoría el documento a descargar [6].

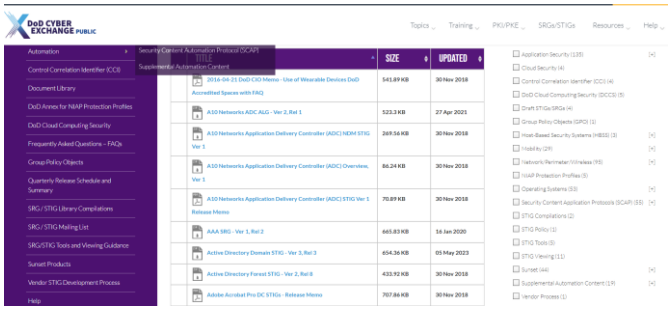

Fig. 2 Página de descarga SGTI

B. CIS – Centro de seguridad de internet

Fig. 3 Logo Cenro de Seguridad de internet

El centro de seguridad de internet es una organización sin fines de lucro impulsada por la comunidad, es responsable de mantener los Benchmarks (puntos de referencia) actualizados con las mejores prácticas reconocidas a nivel mundial pata proteger los sistemas y datos de TI [7]

Los controles CIS son desarrollados por una comunidad de expertos en TI que provienen de una amplia gama de sectores que incluyen retail, fabricación, salud, gobierno, defensa entro otros y cuentan con recomendaciones prescriptivas para más de 25 familias de productos de proveedores.

Los Benchmarks están disponibles en la pagina oficial de la CIS donde se encuentran categorizados para facilitar su descarga. [8]

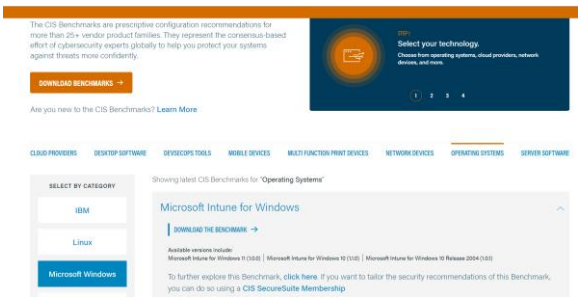

Fig. 4 Página de descarga benchmarks

C. Microsoft cloud security Benchmark

Fig. 5 Logo Microsoft

El bechmark (punto de referencia) de seguridad en la nube de Microsoft (MCSB) proporciona mejores prácticas y recomendaciones para ayudar a mejorar la seguridad de las cargas de trabajo, los datos y los servicios en Azure y su entorno de múltiples nubes. Se centra en las áreas de la nube con información de un conjunto de guías de seguridad holísticas de Microsot que incluyen [9]:

- Marco de adopción de la nube
- Marco de buena arquitectura de Azure
- Taller del director de seguridad de la información
- Otros estándares y marcos de mejores prácticas de seguridad en la industria

Los Benchmarks están disponibles en la página oficina de Microsoft [9]

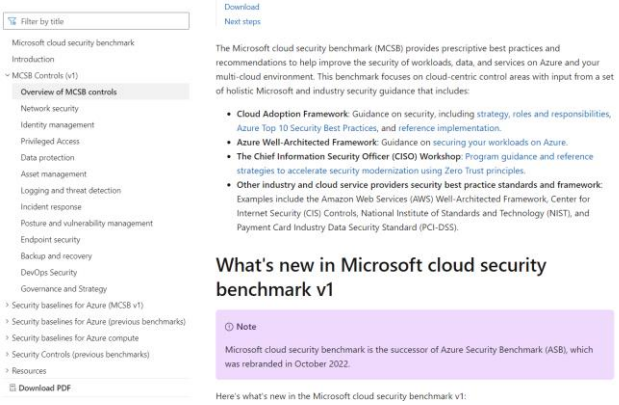

Fig. 6 Pagina descarga bechmark

VII. HERRAMIENTAS PARA REALIZAR HARDERING

Realizar un proceso de endurecimiento a sistemas requiere de conocimiento en cuanto a protocolos y funcionamiento de este. Existen diversas herramientas y lineamientos que informan al usuario las posibles brechas de seguridad encontradas e indican como remediarlas. Es importarte contar con ambientes de pruebas para realizar estas configuraciones antes de implementarlas en ambientes productivos para asir verificar el impacto de la aplicación de estas.

Existen en internet herramientas gratuitas que permiten realizar las configuraciones y posibles remediaciones para obtener un endurecimiento del sistema, este tipo de herramientas generan reportes para que el usuario de forma manual realice el aseguramiento.

A. CIS-CAT LITE

Fig. 7 Logo CIS-CAT Lite

CIS-CAT Lite es una herramienta de evaluación gratuita desarrollada por el CIS (Centro de Seguridad de Internet) la cual ayuda a los usuarios a implementar configuraciones seguras para múltiples tecnologías. [10]

Con CIS-CAT Lite se puede fácilmente:

- Verificar los sistemas contra los bechmark de CIS
- Recibir puntuación de cumplimiento de 1 a 100
- Seguir los pasos de remediación sugeridos para mejorar la seguridad

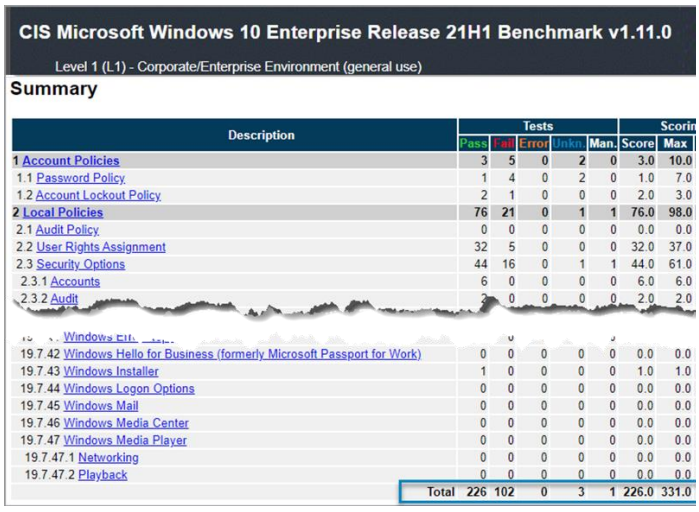

Fig. 8 Reporte generado por CIS-CAT Lite

B. AuditTAP

FB PRO GMBH
System Hardening & Data Protection

Fig. 9 Logo casa matriz de AuditTAP

AuditTAP verifica varios productos estándar para las configuraciones de seguridad importantes y relevantes. Las referencias que se auditan son estándares de seguridad establecidos y probados, por ejemplo, las recomendaciones especificadas en [11]:

- DISA (Agencia de Sistemas de Información de Defensa)
- CIS (Centro para la Seguridad de Internet)
- BSI (Oficina Federal Alemana para la Seguridad de la Información)
- ACSC (Centro Australiano de Seguridad Cibernética)
- Recomendaciones de proveedores, por ejemplo, Microsoft

AuditTAP provee un software para la versión libre el cual al finalizar la auditoria genera un informe en HTML en este se puede ver qué configuraciones cumplen con las recomendaciones y cuáles no.

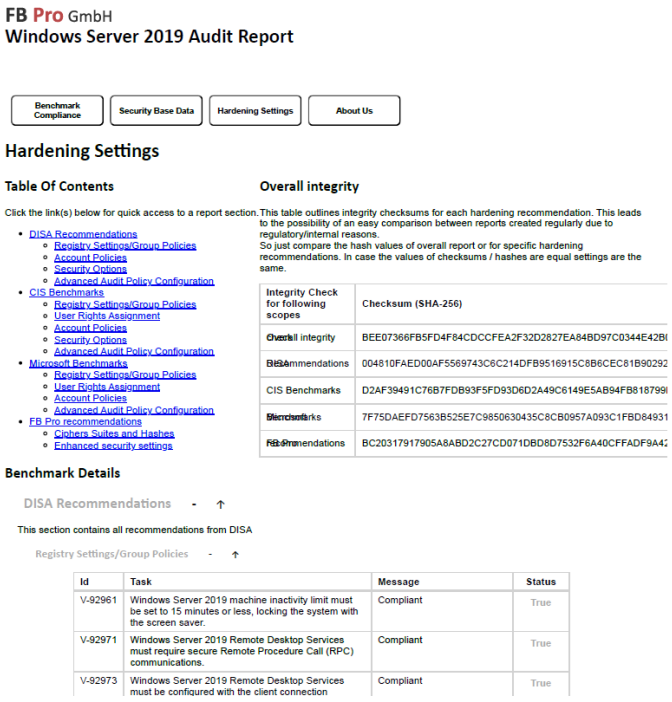

Fig. 10 Reporte generado por AuditTAP

VIII. LABORATORIO DE HARDENIZACIÓN

En este laboratorio se realizará el proceso de hardenización a un sistema operativo Windows Server 2019 estándar en idioma inglés con una configuración base de fábrica, este laboratorio utilizará los siguientes recursos los cuales pueden ser descargados e implementados de forma gratuita.

1. Sistema Operativo Windows Server 2019 en Ingles
2. Sistema de virtualización Virtual Box
3. Software de Hardenización AuditTab

A. Windows Server 2019

Windows Server es una distribución de Microsoft para el uso de servidores. Está desarrollado en lenguaje de programación C++ y Asembler. Se trata de un sistema multiproceso y multiusuario que es utilizado por millones de empresas de todo el mundo gracias a los roles y características ofrece.[12]

Entre los principales roles que ofrece el sistema operativo podemos destacar:

- Directorio Activo
- Virtualización – Hyper-V
- Escritorio Remoto
- DHCP
- DNS
- Webserver

Existen diferentes versiones de Windows server 2019 entre las cuales podemos mencionar:

- Windows server 2019 Essentials: Para pequeñas empresas con un máximo de 25 usuarios y 50 dispositivos.
- Windows server 2019 Standard: Para entornos físicos o mínimamente virtualizados
- Windows server 2019 Datacenter: Para entornos cloud y centro de datos con una gran virtualización [13]

Para instalar este sistema operativo es necesario contar mínimo con los siguientes requisitos:

- Procesador a 1.4 GHz de 64 bits
- Memoria RAM de 512 Mb o 2 GB para el servidor con opción de instalación de experiencia de escritorio (entorno gráfico)
- 32 Gb de espacio en disco duro [14]

Para obtener el medio de instalación de evaluación del sistema operativo Windows Server 2019, se debe ingresar a la dirección web https://www.microsoft.com/es-es/evalcenter/download-windows-server-2019 en el site se encuentra disponible la descarga de la imagen ISO como de la máquina virtual en formato VHD. Para este laboratorio se utilizará la imagen ISO en idioma inglés.

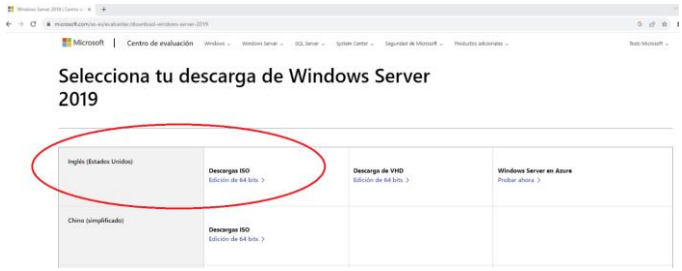

Fig.11 Descarga del sistema operativo desde el site de Microsoft

Para descargar el archivo se debe dar clic sobre el hipervínculo edición de 64 bits, el archivo descargado corresponde a la versión de prueba del sistema operativo el cual se moverá de la carpeta de descargas, en este caso a la carpeta destinada para el laboratorio.

Fig.12 Descarga en la carpeta del laboratorio

B. Software de Virtualización Oracle VirtualBox

VirtualBox es un software desarrollado por Oracle Corporation que permite la ejecución de máquinas virtuales con diferentes características, como sistema operativo, capacidad de disco duro o memoria RAM, entre otras. De este modo, es posible ejecutar programas y funciones en dichas maquinas sin afectar al dispositivo real en el que se ejecute. VirtualBox es muy utilizado para probar el comportamiento de sistemas operativos y programas frente a aspectos relacionados de ciberseguridad como la instalación de parches de seguridad y endurecimiento de estos. [15]

Algunas de las ventajas de utilizar VirtualBox son:

- Es gratuito
- Alto nivel de portabilidad
- Fácil de descargar y utilizar
- Interface Amigable
- Múltiples sistemas operativos pueden ser instalados como Windows o Linux

Para instalar VirtualBox en Windows es necesario contar mínimo con los siguientes requisitos:

- Procesador a 1 GHz de 64 bits
- Memoria RAM de 512 Mb
- 15 Gb de espacio en disco duro [16]

Para obtener la última versión de VirtualBox se debe ingresar a https://www.oracle.com/co/virtualization/technologies/vm/downloads/virtualbox-downloads.html?source=:ow:o:p:nav:mmddyyVirtualBoxHero_co&intcmp=:ow:o:p:nav:mmddyyVirtualBoxHero_co.

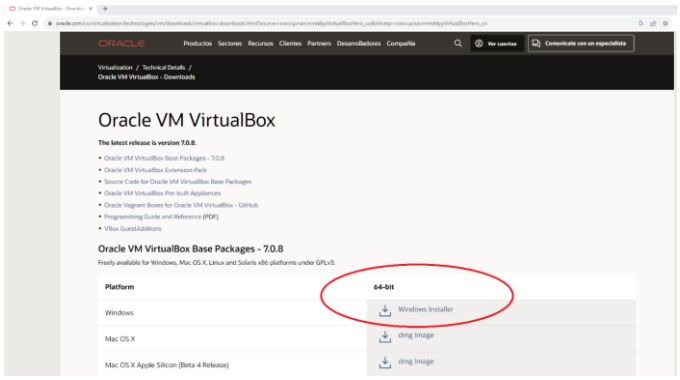

Fig.13 Descarga del sistema operativo desde el site de Microsoft

Para descargar el archivo se debe dar clic sobre el hipervínculo Windows Installer de la plataforma Windows, el archivo descargado se moverá de la carpeta de descargas a la carpeta destinada para el laboratorio.

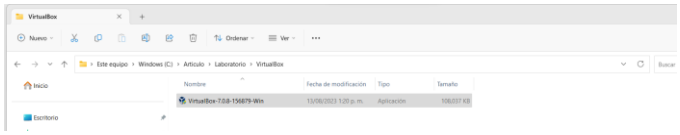

Fig.14 Archivo en la carpeta del laboratorio

C. *Software de Hardenización – AuditTab*

Como parte del análisis de herramientas realizado en este artículo, se utilizará la herramienta AuditTap para el ejercicio de endurecimiento del sistema operativo Windows server 2019.

La herramienta se debe descargar del link https://github.com/fbprogmbh/Audit-Test-Automation donde encontraremos la última versión.

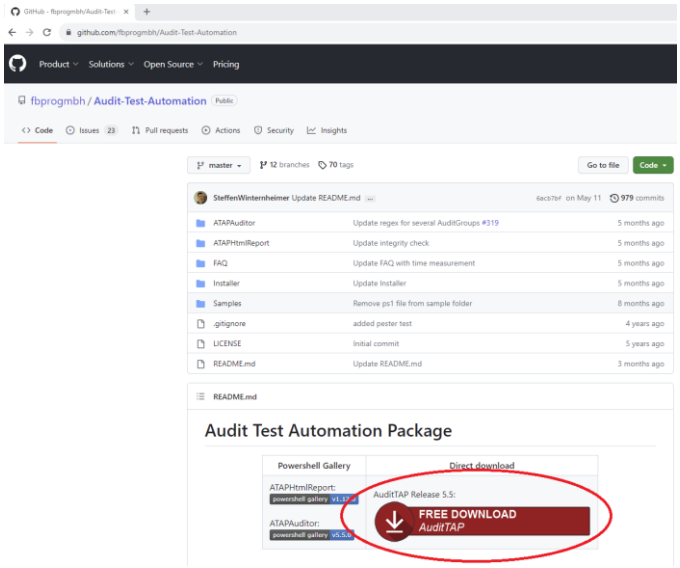

Fig.15 Descarga del software AuditTab

Para descargar el archivo se debe dar clic sobre el hipervínculo Free Download AuditTAP, el archivo descargado se moverá de la carpeta de descargas a la carpeta destinada para el laboratorio.

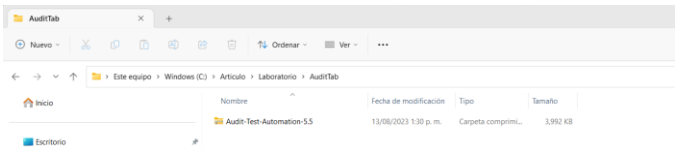

Fig.16 Movimiento del archivo a la carpeta del laboratorio

Una vez descargado el software necesario procederemos con el laboratorio llevando a cabo los siguientes pasos:

- Instalación de VirtualBox
- Instalación del Sistema Operativo Windows Server 2019
- Instalación de Audittap
- Configuración y ejecución de AuditTap
- Generación y revisión del reporte
- Remediación de algunas vulnerabilidades encontradas
- Generación y revisión del Reporte

Este laboratorio será ejecutado en un equipo con las siguientes características:

- Windows 11 Pro
- Memoria Ram 16 GB
- Disco Duro 2556 Gb

Fig.17 Características técnicas del equipo host para el laboratorio

D. *Instalación de VirtualBox*

Los siguientes son los pasos para realizar la instalación de VirtualBox

1. En la carpeta donde se encuentra el instalador daremos doble click sobre el archivo.

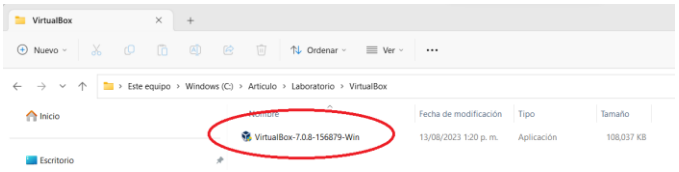

Fig.18 Paso 1 instalación de VirtualBox

El sistema iniciará la instalación de la aplicación.

2. Se desplegará la pantalla de bienvenida a la instalación donde se debe dar click al botón next.

Fig.19 Paso 2 instalación de VirtualBox

3. El sistema solicitara la selección de los componentes a instalar al igual que la ruta de instalación del aplicativo, para el ejercicio daremos click en el botón next.

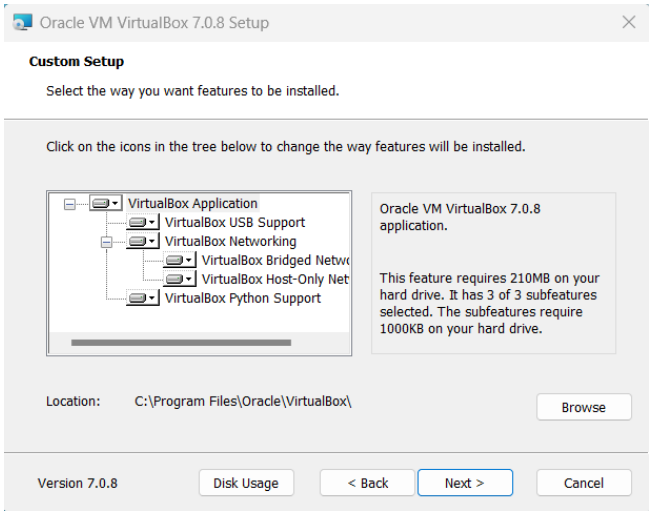

Fig.20 Paso 3 instalación de VirtualBox

4. El proceso de instalación indicará que debe instalar componentes de red para lo cual temporalmente se presentará una desconexión de la red, en esta pantalla deberemos dar click en yes.

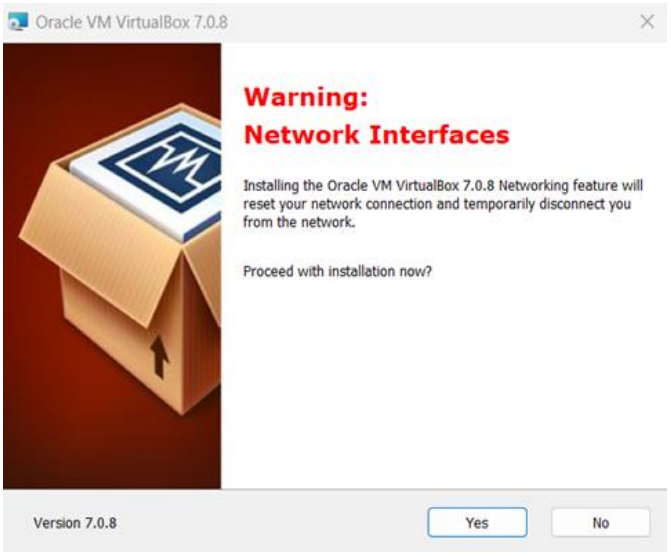

Fig. 21 Paso 4 instalación de VirtualBox

5. El proceso de instalación notifica que debe instalar componentes de python y librerías adicionales de Windows, daremos click en el botón yes para continuar.

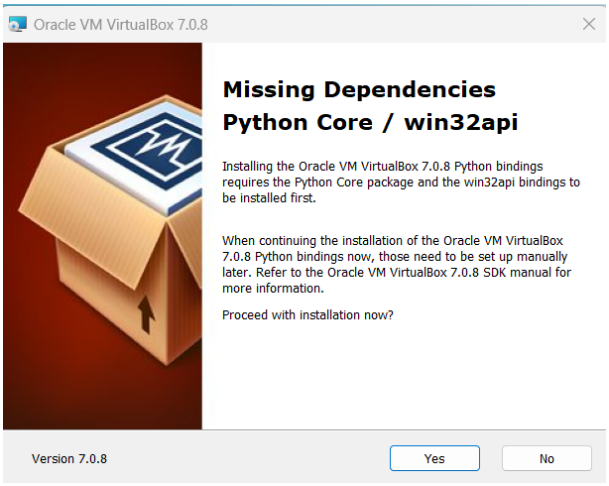

Fig. 22 Paso 5 instalación de VirtualBox

6. Una vez llegado a este punto el sistema indicará que está listo para iniciar la instalación. Se debe dar click en el botón install para iniciar el proceso.

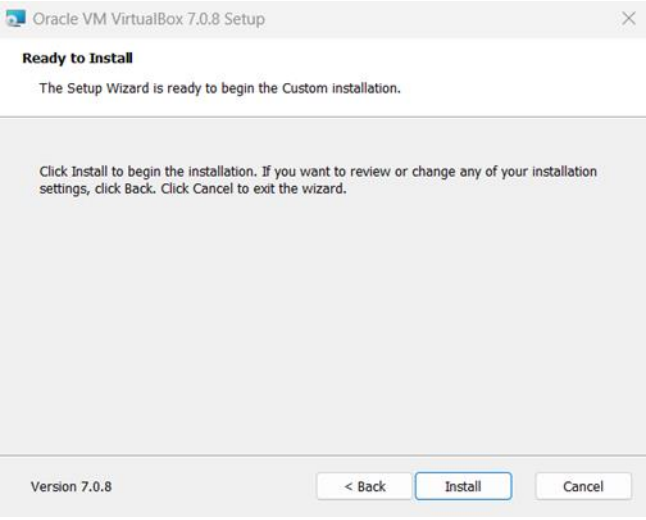

Fig. 23 Paso 6 instalación de VirtualBox

7. Se iniciará el proceso de instalación.

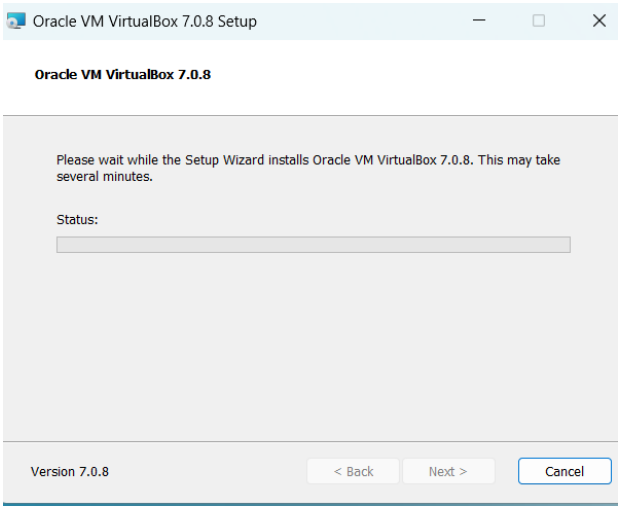

Fig. 24 Paso 7 instalación de VirtualBox

8. Cuando finalice la instalación el sistema informará y dará la posibilidad de iniciar el aplicativo. En esta pantalla pulsaremos sobre el botón finish.

Fig. 25 Paso 8 instalación de VirtualBox

E. Instalación de Windows Server 2019

Para la instalación de Windows Server 2019, iniciaremos el software de virtualización Virtual Box instalado con anterioridad, para lo cual daremos doble click sobre el icono instalado en el escritorio.

Fig. 28 ícono de VirtualBox

1. Una vez este en ejecución del virtualizador seleccionamos la opción Nuevo:

Fig. 29 Paso 1 instalación de Windows server 2019

2. Diligenciamos la información que nos solicita el sistema así:

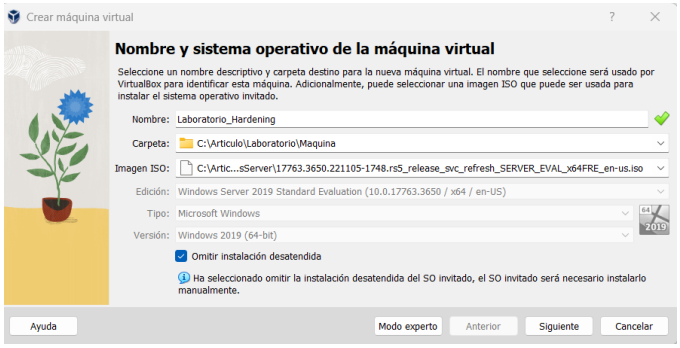

Fig. 30 Paso 2 instalación de Windows server 2019

Pulsamos en siguiente.

3. Seleccionamos los recursos de hardware que serán asignados a la máquina virtual:

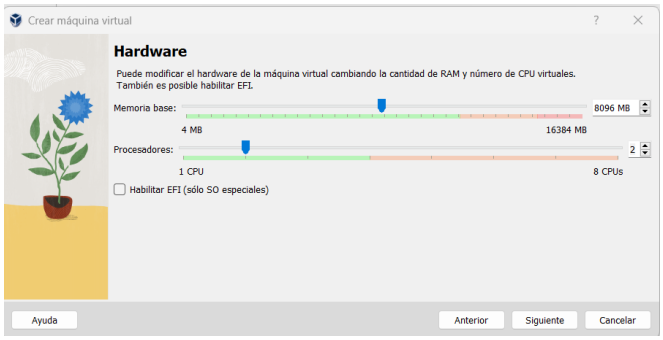

Fig. 31 Paso 3 instalación de Windows server 2019

Pulsamos en siguiente.

4. Indicaremos la cantidad de gigas que serán asignadas al disco duro virtual de la máquina virtual.

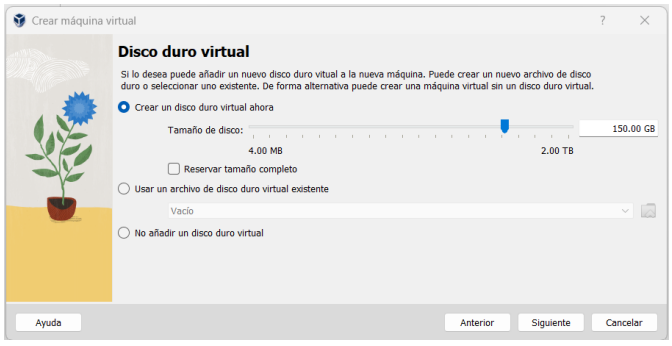

Fig. 32 Paso 4 instalación de Windows server 2019

Pulsamos en siguiente.

5. El sistema mostrará un resumen de las características técnicas definidas.

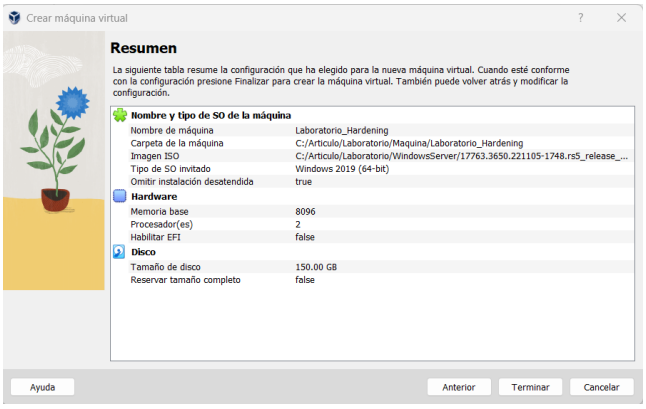

Fig. 33 Paso 5 instalación de Windows server 2019

Pulsamos en terminar.

6. En este punto el sistema virtualbox cuenta con las definiciones necesarias a nivel de máquina virtual. Procederemos a instalar Windows Server 2019 sobre esta definición.

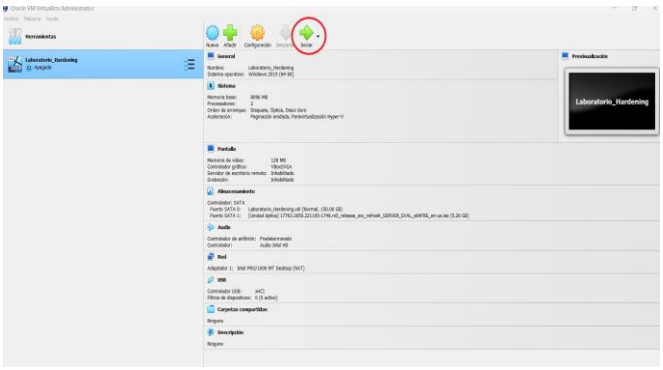

Fig. 34 Paso 6 instalación de Windows server 2019

Pulsamos sobre el botón Iniciar.

7. Se desplegará la ventana del equipo virtual mostrando el inicio de la instalación de Windows server 2019.

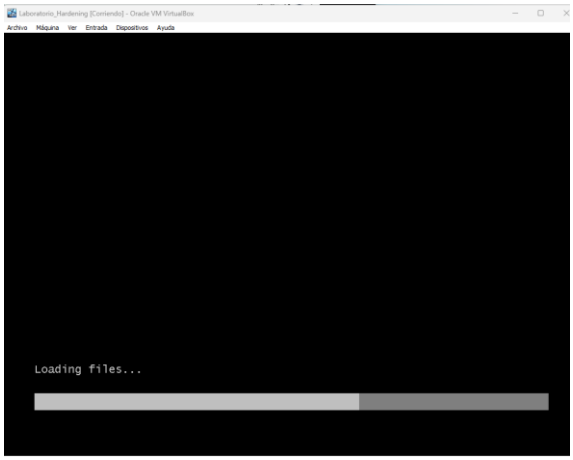

Fig. 35 Paso 7 instalación de Windows server 2019

8. El instalador solicitará el lenguaje, formato de tiempo y valor a utilizar al igual que el idioma del teclado, para este laboratorio solo se modificará este último parámetro a teclado latinoamericano.

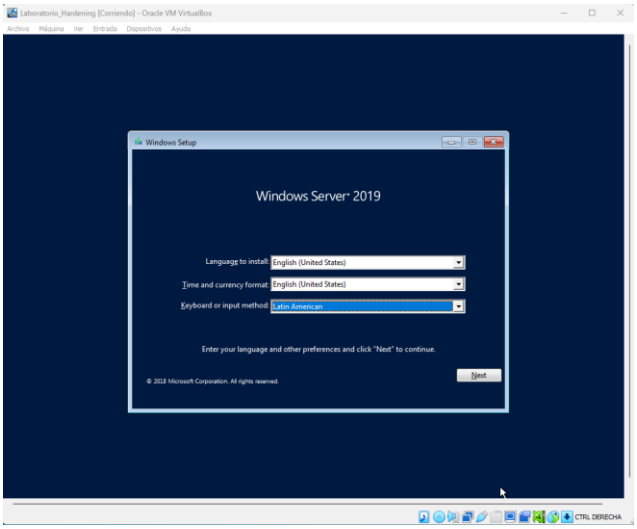

Fig. 36 Paso 8 instalación de Windows server 2019

Pulsamos en next.

9. El sistema nos indica que podemos iniciar con la instalación.

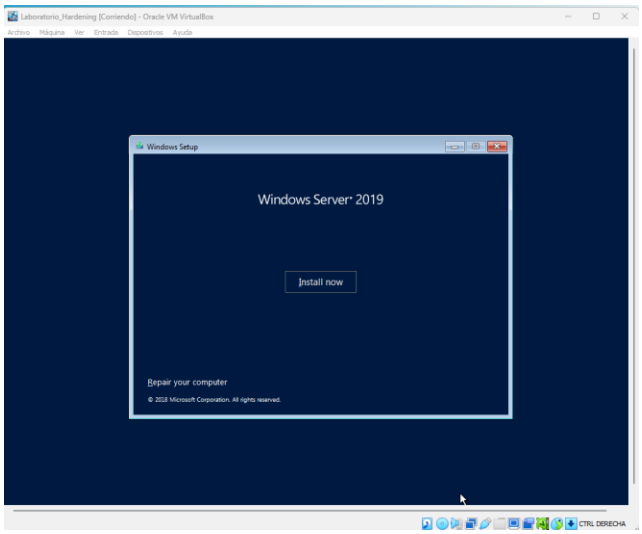

Fig. 37 Paso 9 instalación de Windows server 2019

Pulsaremos en Install now

10. El sistema nos solicita escoger la versión de Windows Server 2019 a instalar, para este laboratorio seleccionaremos Windows Server 2019 Standard Evaluation (Desktop Experience).

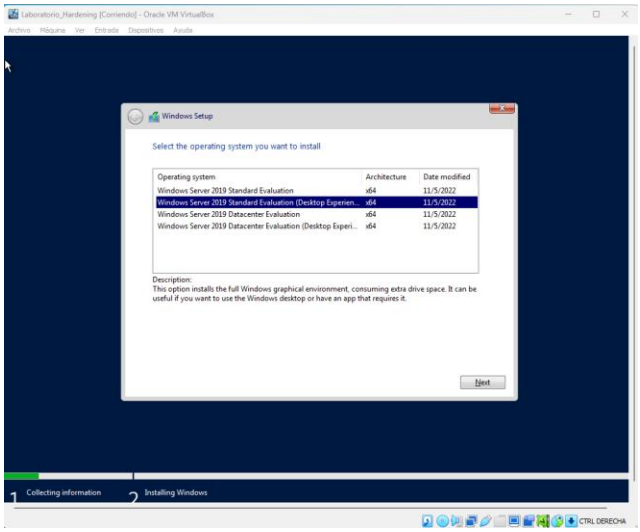

Fig. 38 Paso 10 instalación de Windows server 2019

Pulsamos en next.

11. El instalador solicita aceptar los términos de licencia.

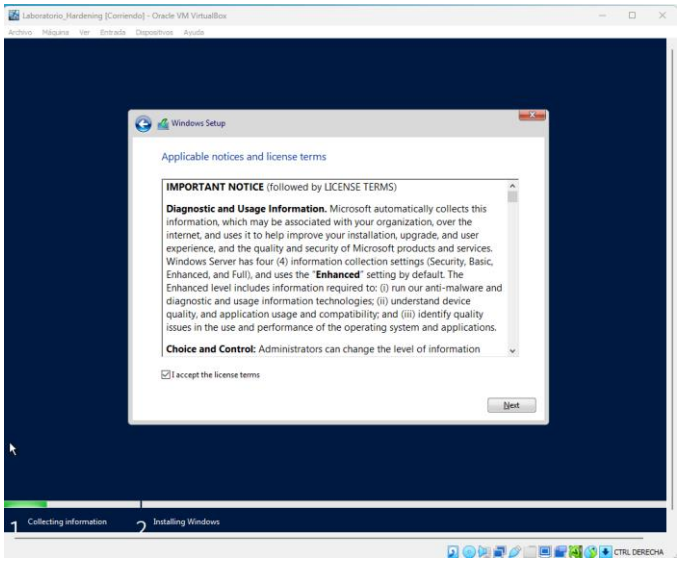

Fig. 39 Paso 11 instalación de Windows server 2019

Seleccionamos next.

12 Debemos indicarle al instalador si es una actualización o una instalación nueva, para este ejercicio seleccionaremos Custom: Install Windows only (advanced).

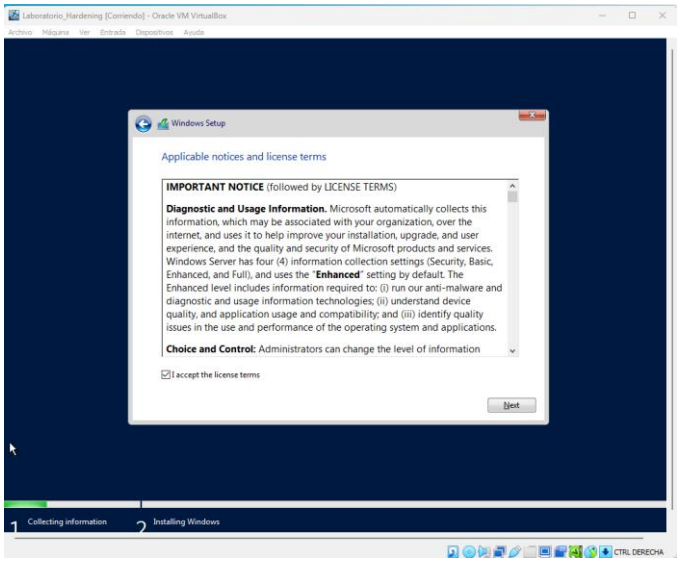

Fig. 40 Paso 12 instalación de Windows server 2019

13. Debemos especificar si utilizaremos la totalidad del disco asignado o realizaremos particiones en el sistema operativo, se dejarán los valores presentados en pantalla.

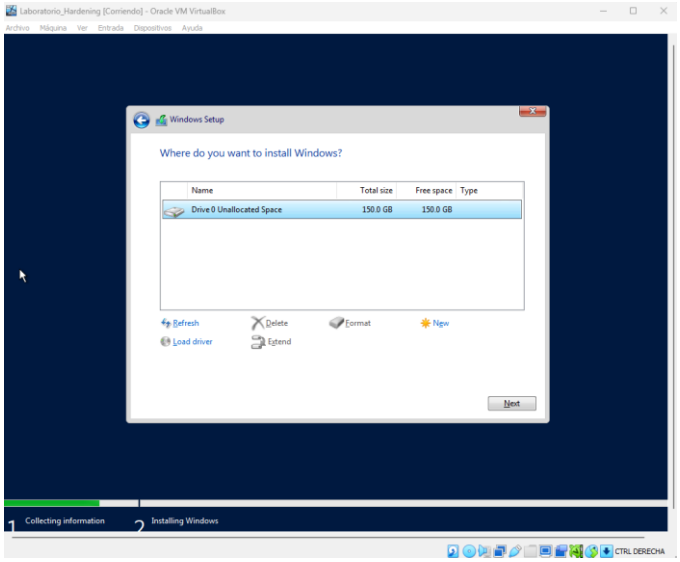

Fig. 41 Paso 13 instalación de Windows server 2019

Seleccionamos next.

14. El instalador inicia con el despliegue del sistema operativo.

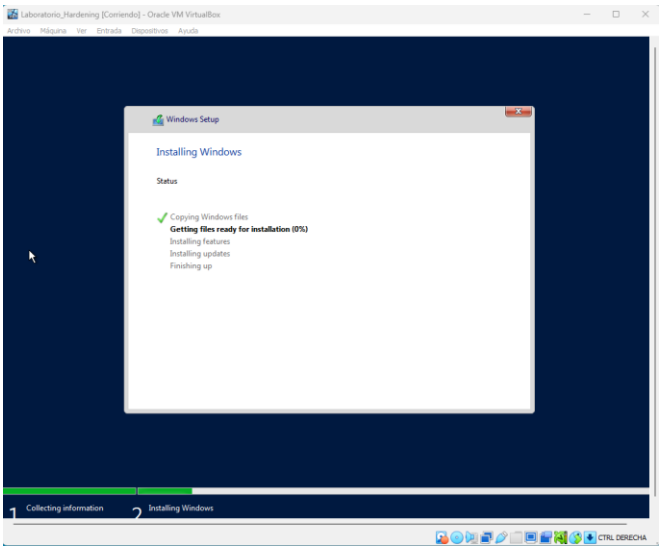

Fig. 42 Paso 14 instalación de Windows server 2019

15. Al finalizar la instalación el sistema se reiniciará.

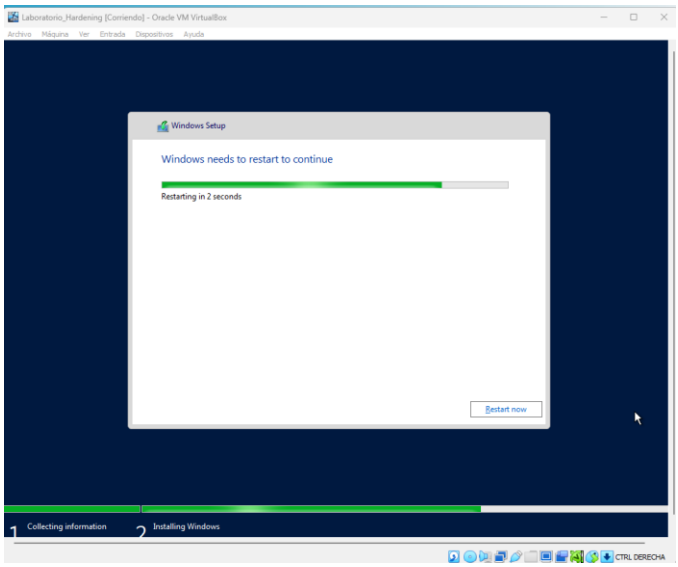

Fig. 43 Paso 15 instalación de Windows server 2019

16. Una vez reiniciado el sistema solicitará la contraseña del usuario administrator.

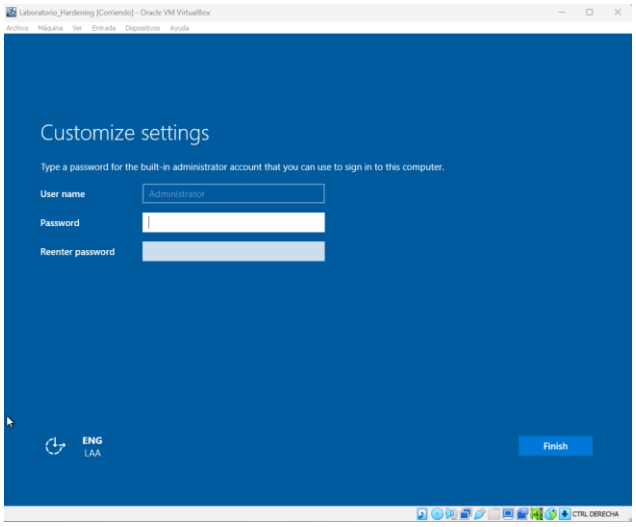

Fig. 44 Paso 16 instalación de Windows server 2019

Al configurar la contraseña seleccionamos finish.

17. El instalador ha finalizado con el proceso y el sistema operativo ya se encuentra disponible.

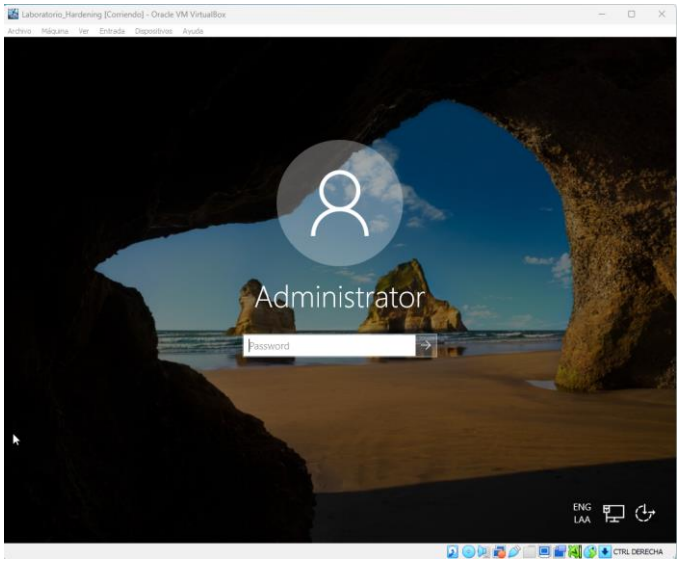

Fig. 45 Paso 17 instalación de Windows server 2019

F. Instalación de AuditTab

1. Ingresamos al sistema operativo con el usuario Administrator y la contraseña previamente configurada.

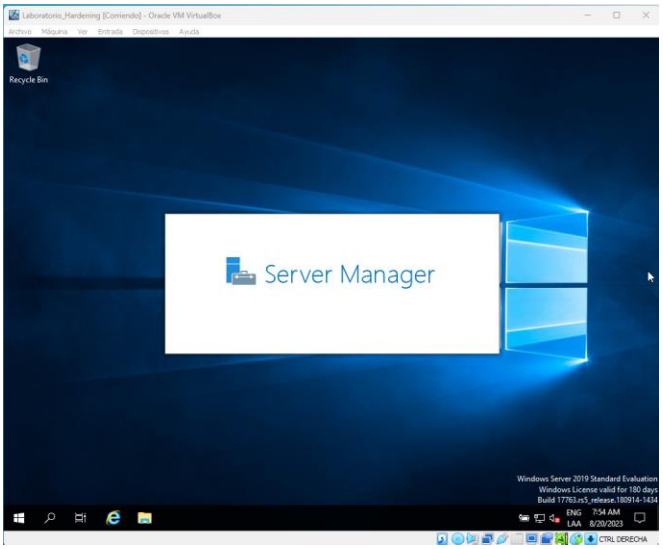

Fig. 46 Paso 1 instalación de AuditTab

2. Creamos una carpeta y en esta copiamos el instalador de AuditTab descargado previamente.

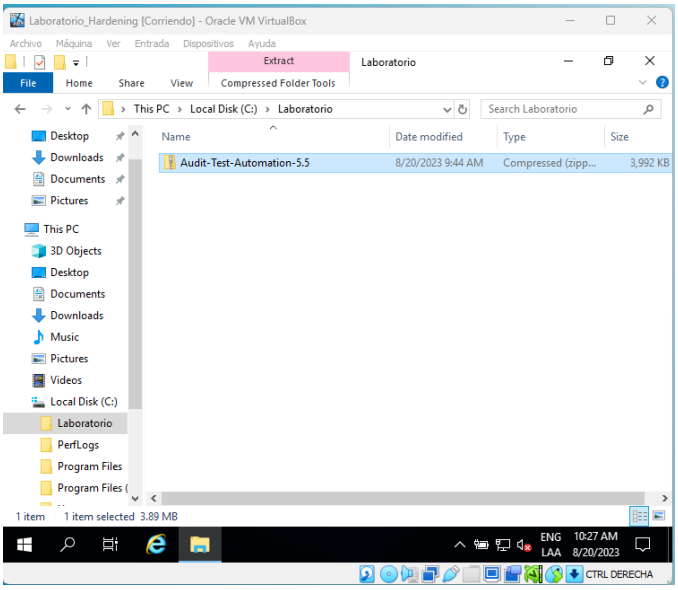

Fig. 47 Paso 2 instalación de AuditTab

3. Procedemos a descomprimir el archivo descargado.

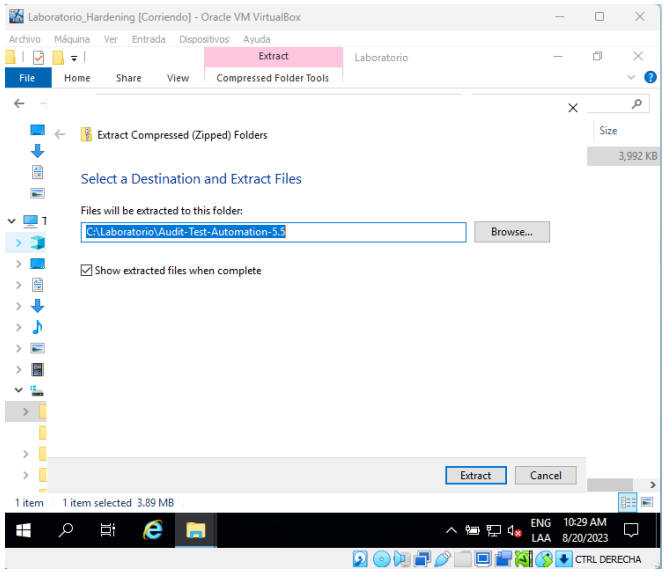

Fig. 48 Paso 3 instalación de AuditTab

4. Ingresamos a la carpeta donde fue descomprimido el archivo y nos ubicamos en la capeta Installer.

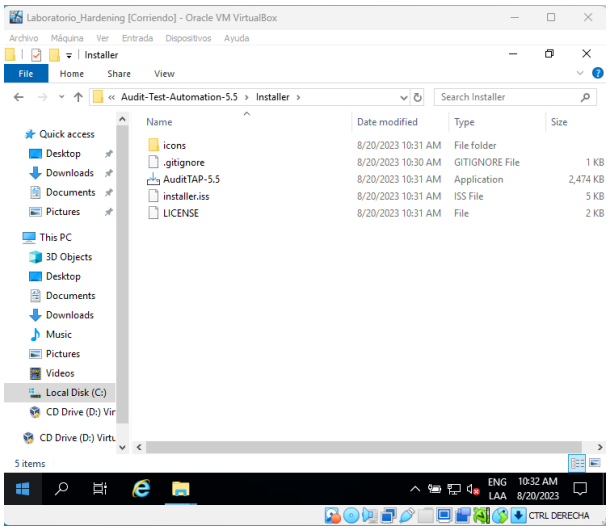

Fig. 49 Paso 4 instalación de AuditTab

5. Ejecutamos el archivo AuditTAP-5.5 con privilegios de Administrador

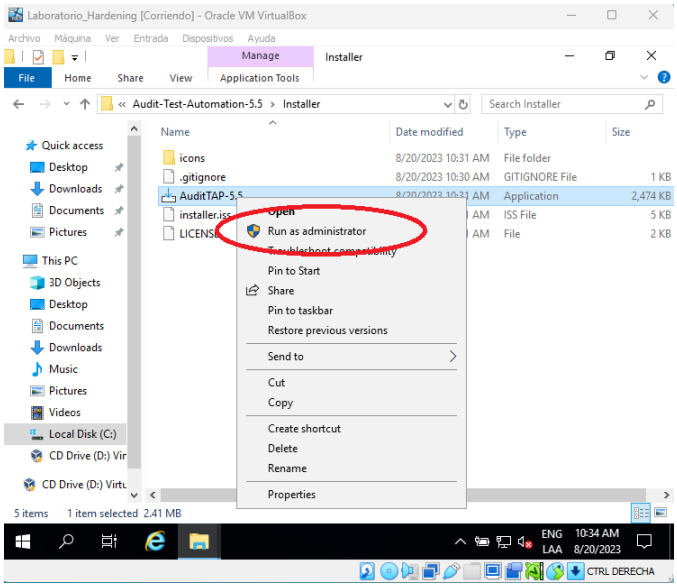

Fig. 50 Paso 5 instalación de AuditTab

6. Aceptamos la licencia del producto

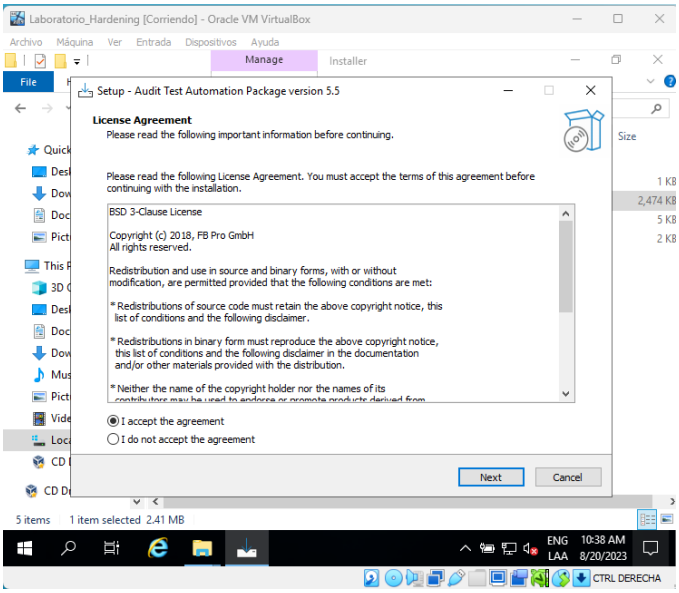

Fig. 51 Paso 6 instalación de AuditTab

Seleccionamos next.

7. Seleccionamos la carpeta donde se realizará la instalación, se recomienda dejar el valor sugerido.

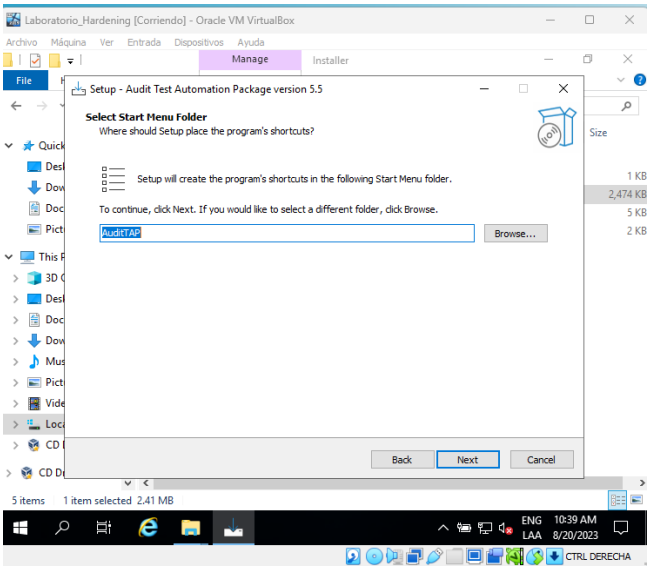

Fig. 52 Paso 7 instalación de AuditTab

Seleccionamos next

8. El instalador solicita especificar la versión a utilizar y nos brinda dos opciones, la versión estable la cual es la recomendada o la versión que se encuentra en desarrollo, se debe escoger la versión estable.

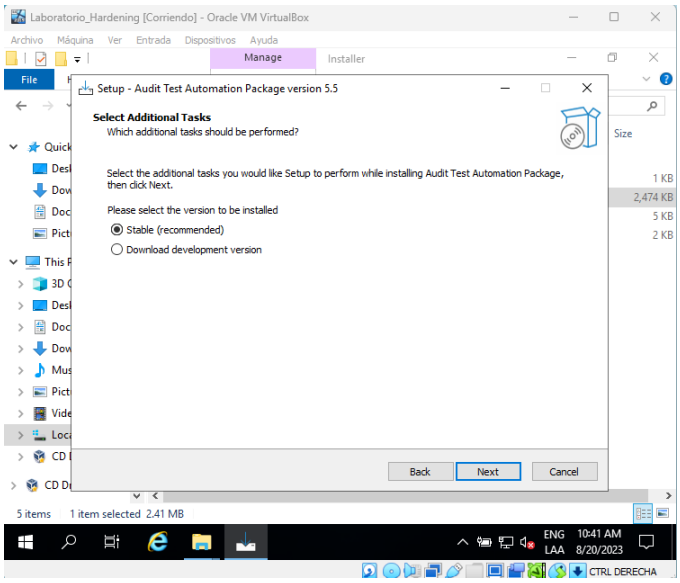

Fig. 53 Paso 8 instalación de AuditTab

Seleccionamos next

9. El instalador indica que ya cuenta con la información necesaria para proceder con la instalación.

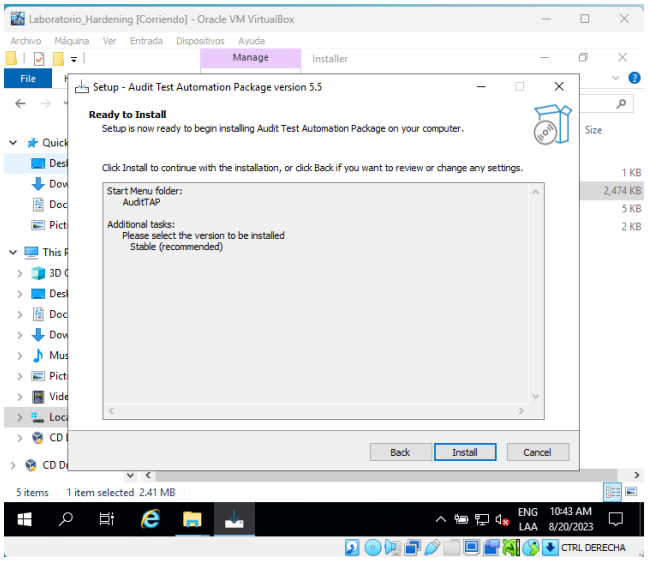

Fig. 54 Paso 9 instalación de AuditTab

Seleccionamos Install

10. Se inicial el proceso de instalación, una vez finalizado el instalador nos informará.

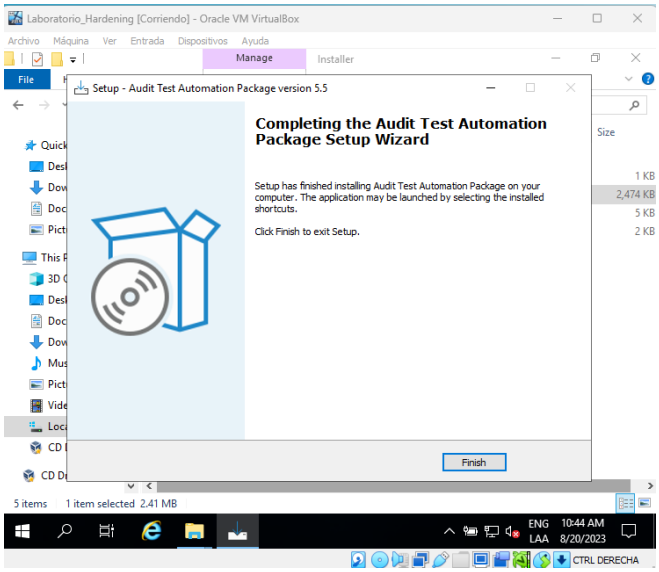

Fig. 55 Paso 10 instalación de AuditTab

Seleccionamos Finish

G. Ejecución del proceso de hardenización en el servidor

Finalizada la instalación de AuditTAB iniciaremos con el proceso de ejecución de la primera revisión del servidor y verificaremos el reporte generado por la herramienta.

1. Se debe desplegar el menú de Windows e ingresar por el icono AudiTAP.

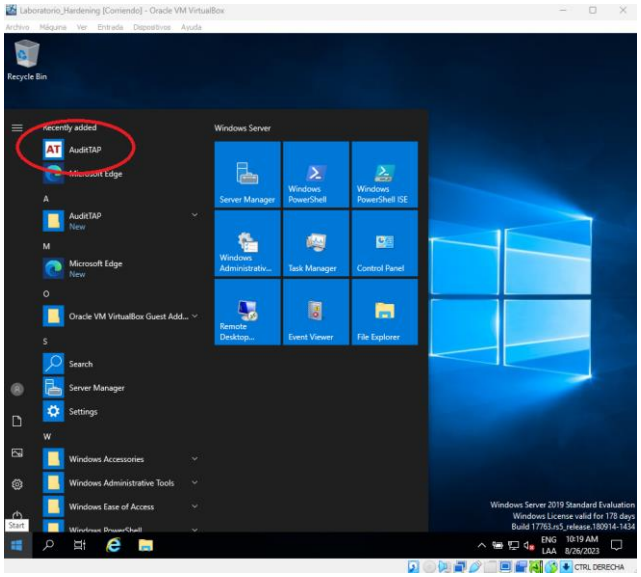

Fig. 56 Paso 1 Proceso de Hardenización

2. El sistema iniciara con el cargue de componentes para después visualizar el menú de opciones.

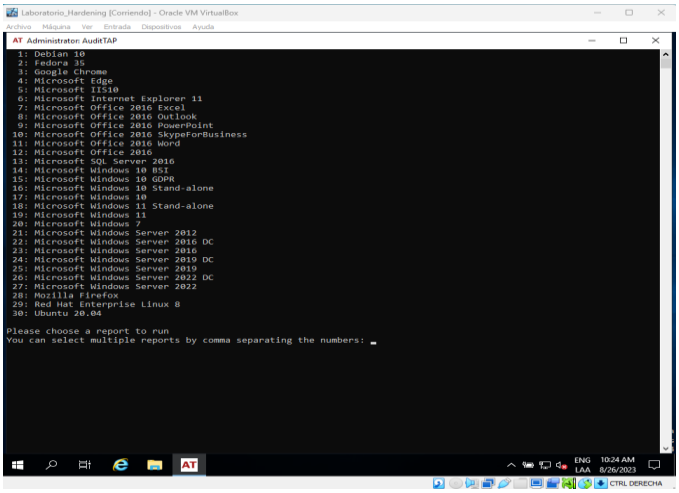

Fig. 57 Paso 2 Proceso de Hardenización

3. Para este laboratorio se seleccionará la opción 25 correspondiente a Microsoft Windows Server 2019

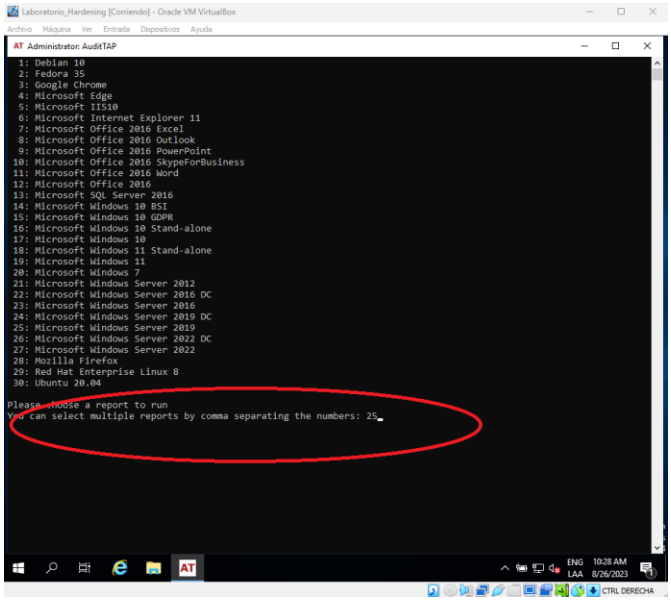

Fig. 58 Paso 3 Proceso de Hardenización

4. Una vez seleccionado la versión del sistema operativo a escanear y pulsar enter, se iniciará el proceso de revisión, este contempla varias fases las cuales serán informadas en pantalla.

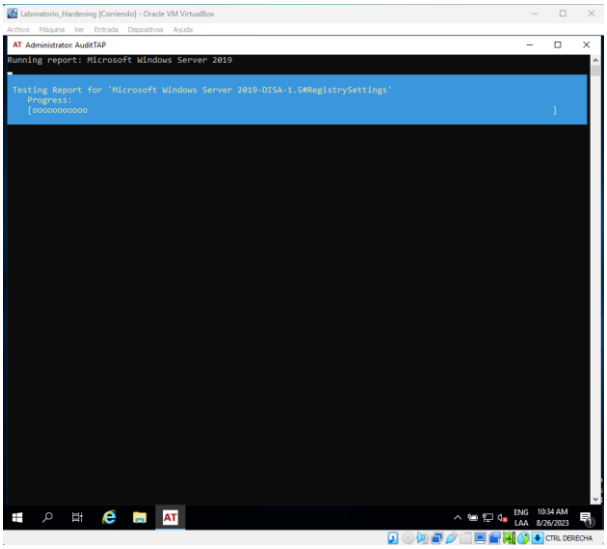

Fig. 59 Paso 4 Proceso de Hardenización

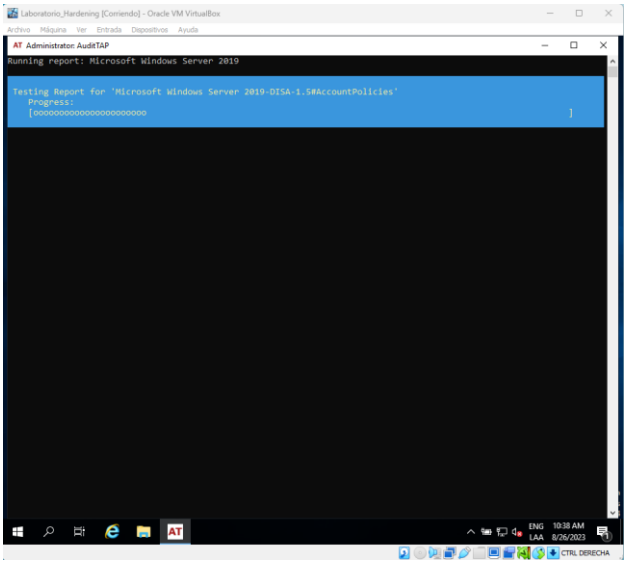

Fig. 60 Paso 4 Proceso de Hardenización

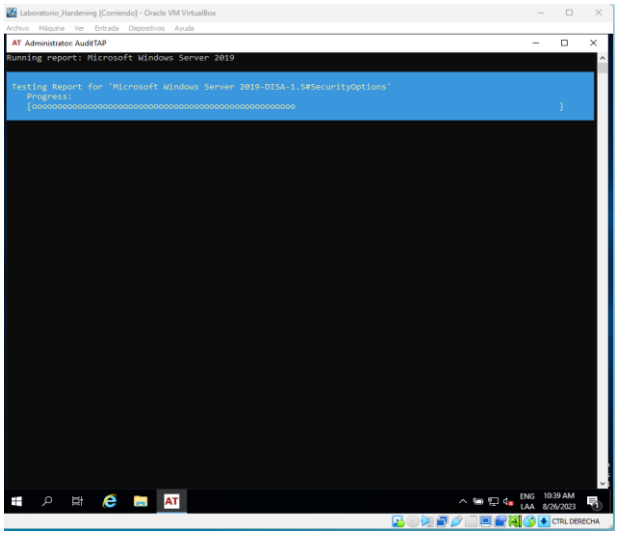

Fig. 61 Paso 4 Proceso de Hardenización

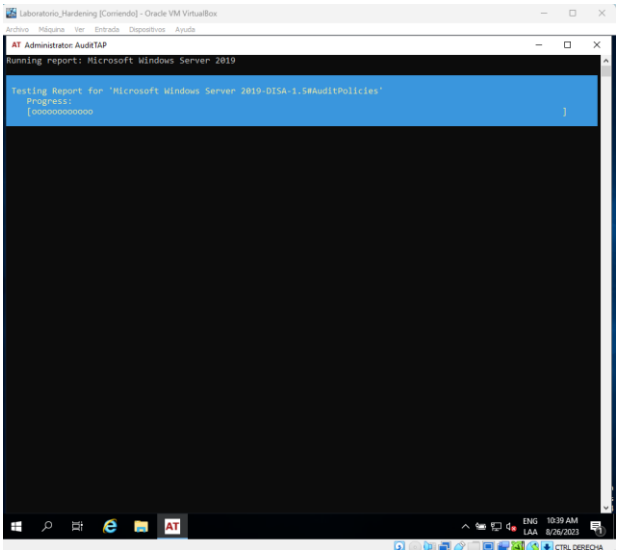

Fig. 62 Paso 4 Proceso de Hardenización

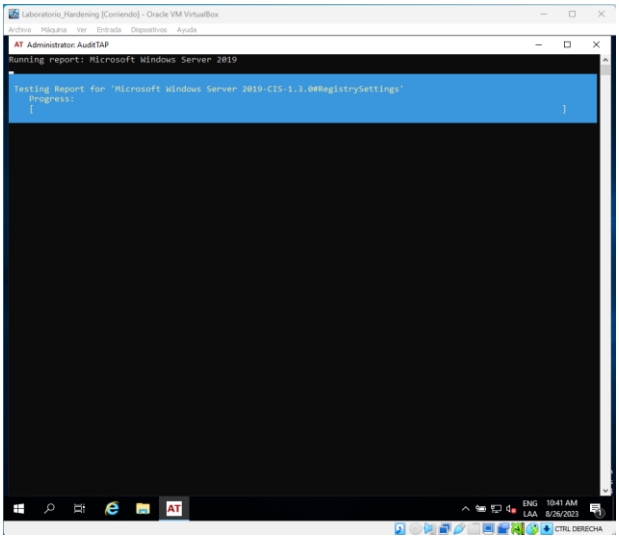

Fig. 63 Paso 4 Proceso de Hardenización

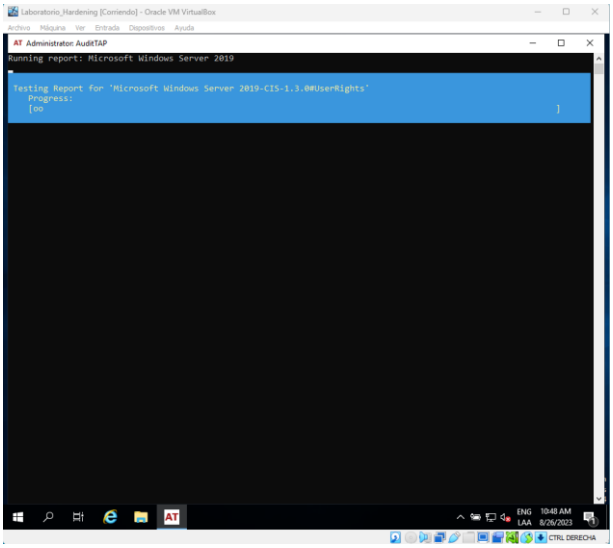

Fig. 64 Paso 4 Proceso de Hardenización

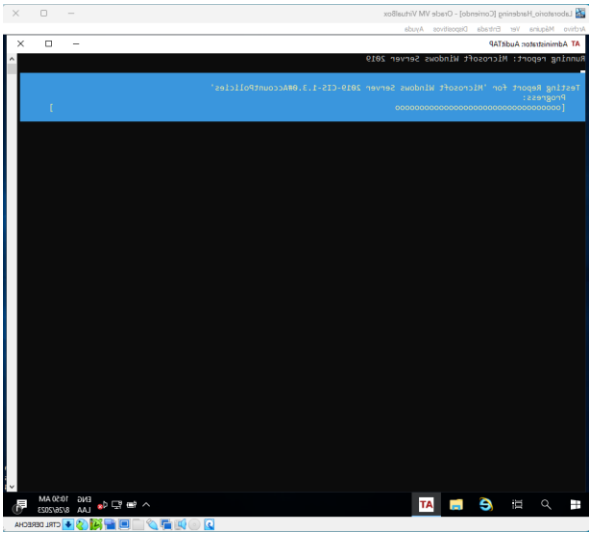

Fig. 65 Paso 4 Proceso de Hardenización

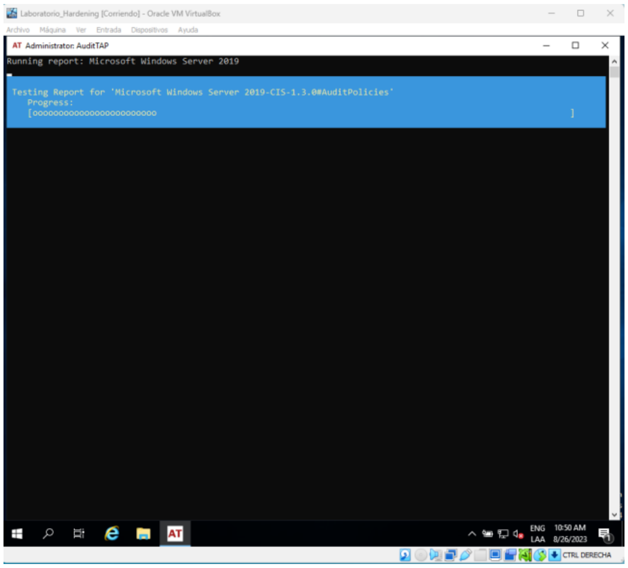

Fig. 66 Paso 4 Proceso de Hardenización

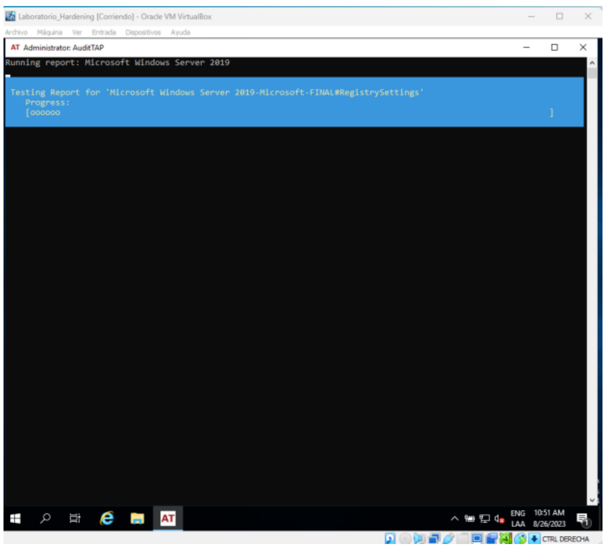

Fig. 67 Paso 4 Proceso de Hardenización

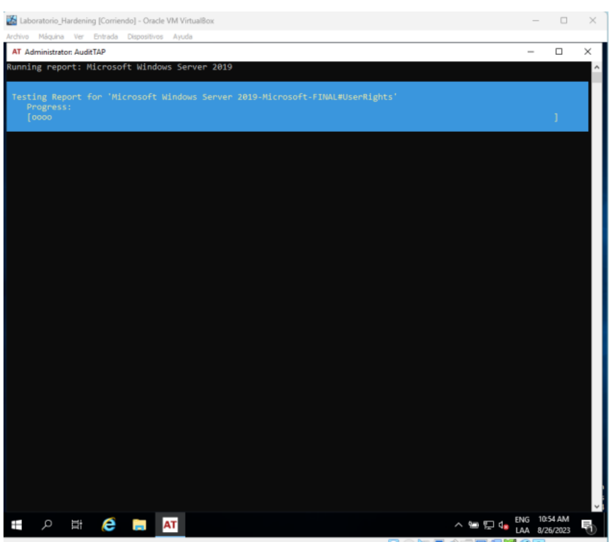

Fig. 68 Paso 4 Proceso de Hardenización

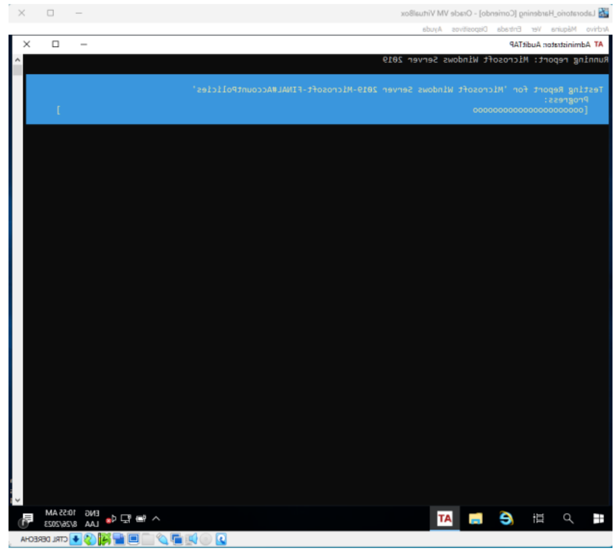

Fig. 69 Paso 4 Proceso de Hardenización

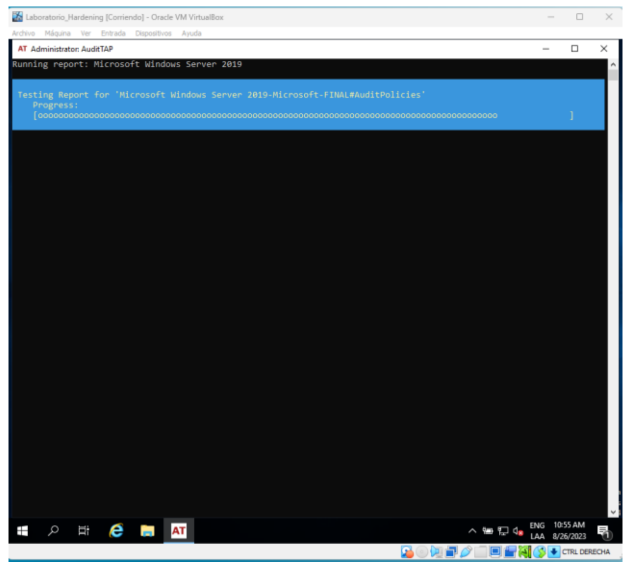

Fig. 70 Paso 4 Proceso de Hardenización

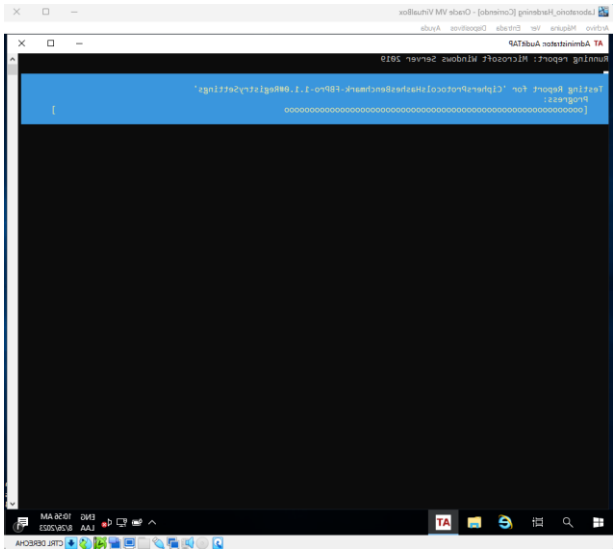

Fig. 71 Paso 4 Proceso de Hardenización

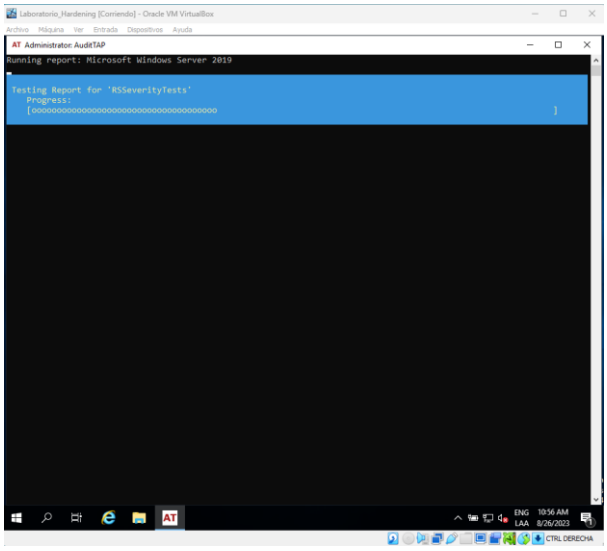

Fig. 72 Paso 4 Proceso de Hardenización

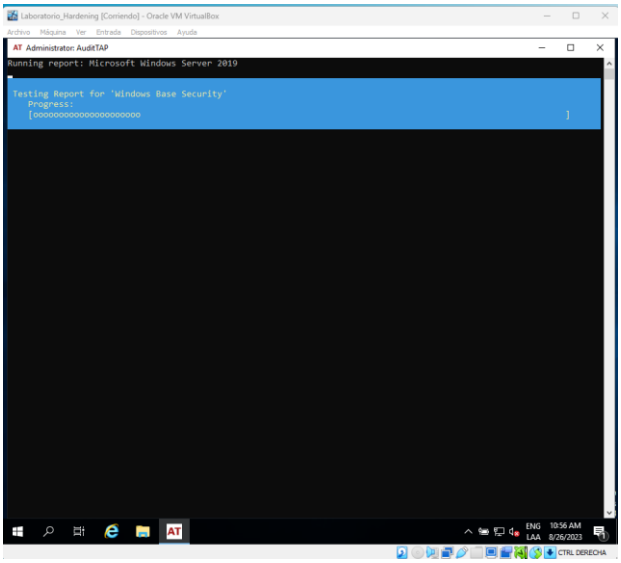

Fig. 73 Paso 4 Proceso de Hardenización

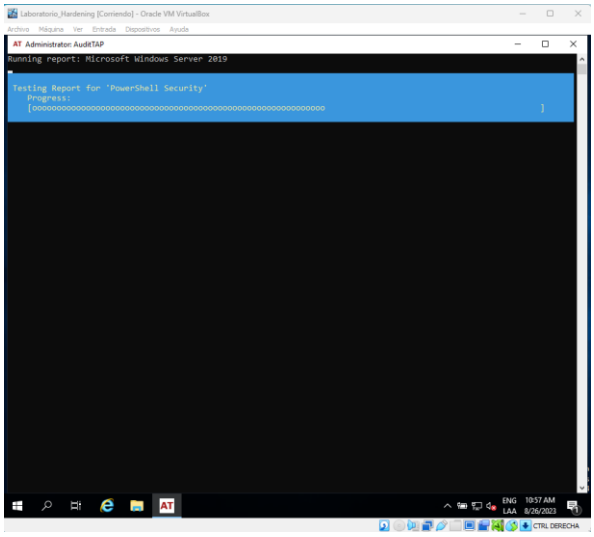

Fig. 74 Paso 4 Proceso de Hardenización

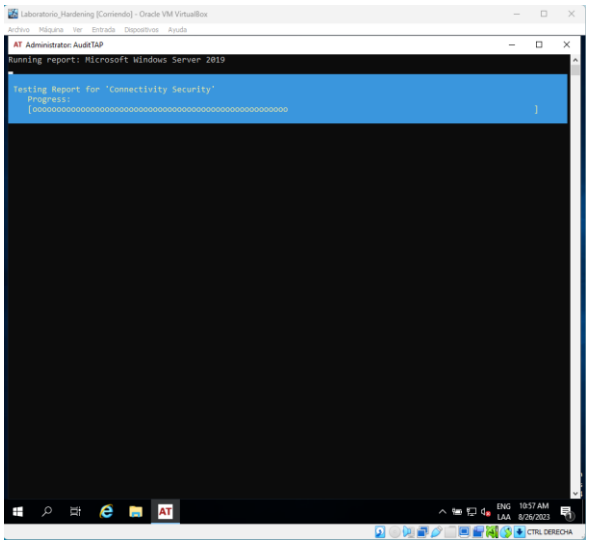

Fig. 75 Paso 4 Proceso de Hardenización

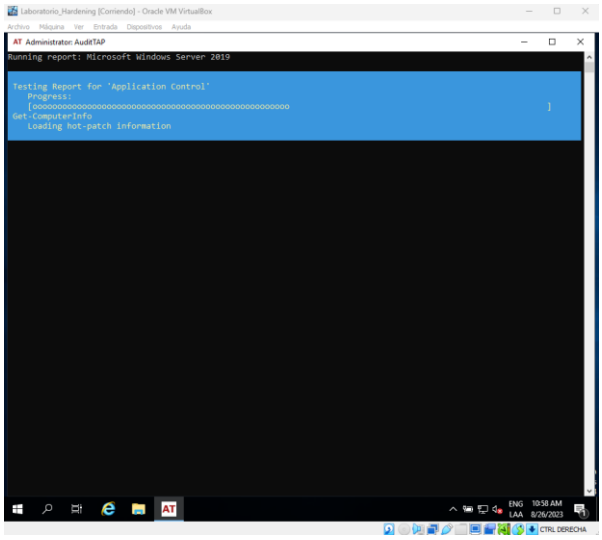

Fig. 76 Paso 4 Proceso de Hardenización

5. Finalizado el proceso el cual dura aproximadamente 25 minutos, el sistema indica si queremos abrir la ubicación del reporte.

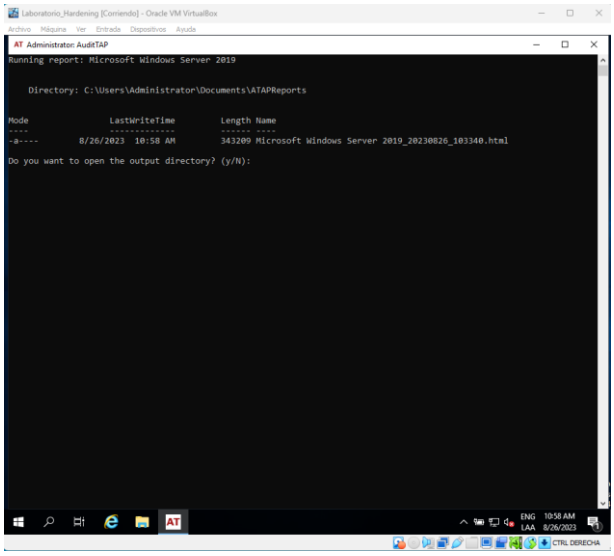

Fig. 77 Paso 5 Proceso de Hardenización

6. En la ubicación del reporte se encuentra un archivo en formato HTML el cual contiene el resultado de la revisión.

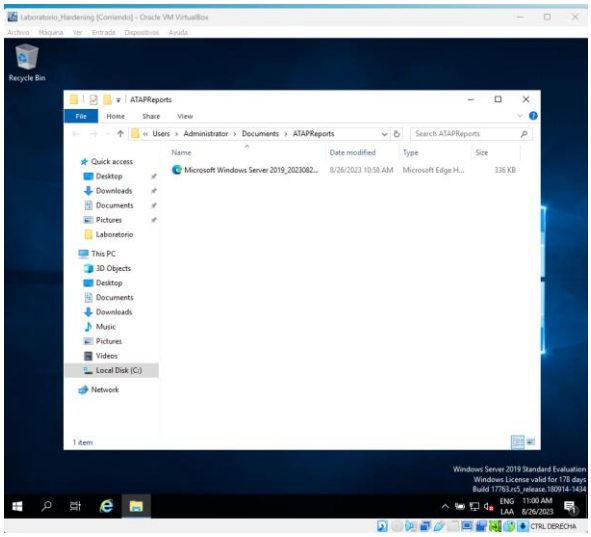

Fig. 78 Paso 6 Proceso de Hardenización

7. El reporte cuenta con cuatro pestañas donde se puede visualizar el resultado de la revisión realizada.

La primera pestaña (Benchmarks Compliance) informa el estado general del sistema de forma consolidada y las calificaciones obtenidas teniendo en cuenta las mejores prácticas de la DISA, CIS Benchmarks, Microsoft Bencmarks y las recomendaciones de la FB Pro.

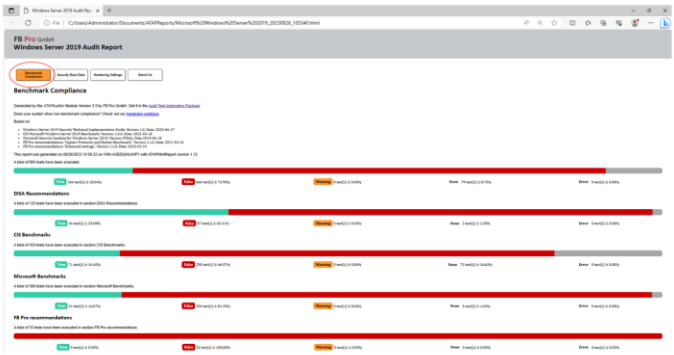

Fig. 79 Paso 7 Proceso de Hardenización pestaña 1

La segunda pestaña informa el estado del sistema según la base de seguridad del producto para los cual realiza revisiones a nivel de la Seguridad de la plataforma, línea base de seguridad de Windows, seguridad frente a PowerShell, seguridad en conectividad y control de aplicaciones.

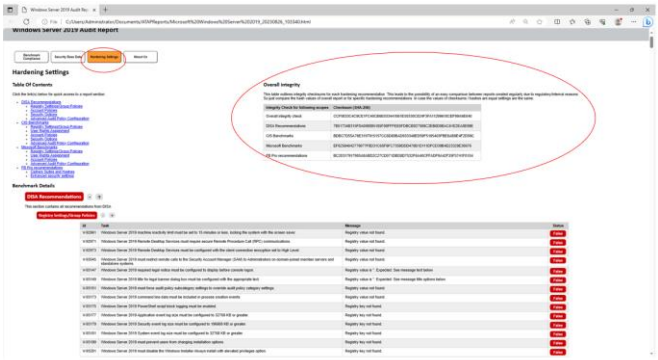

Fig. 80 Paso 7 Proceso de Hardenización pestaña 2

La tercera pestaña informa las configuraciones de hardenización que se deben tener establecidas según las buenas prácticas de la DISA, CIS, Microsoft y FB Pro, cuales están implementadas y cuáles no. Este reporte genera un hash de integridad para evitar modificaciones al mismo por cada tipo de revisión realizada.

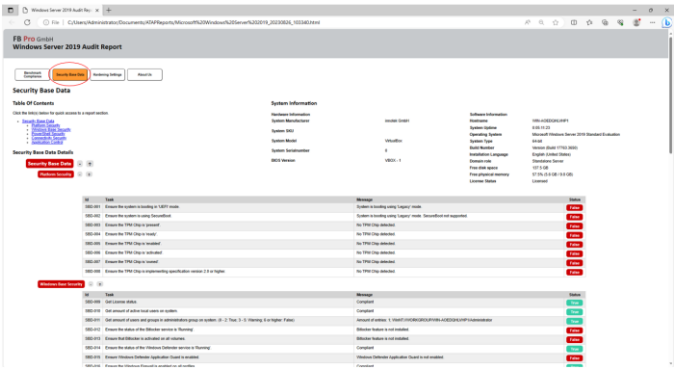

Fig. 81 Paso 7 Proceso de Hardenización pestaña 3

La cuarta y última pestaña, muestra las diferentes versiones del producto para compra.

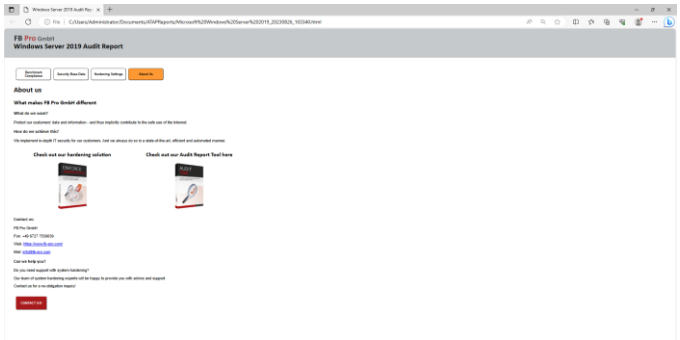

Fig. 82 Paso 7 Proceso de Hardenización pestaña 4

H. Procedimiento de Remediación

Como parte de este laboratorio se realizará la remediación de dos de las novedades encontradas en el apartado de Security Option de la pestaña Hardening Settings.

Fig. 83 Novedades

Estas novedades indican que el usuario Administrator y Guest deben ser renombrados.
Para resolver esta novedad se deben realizar los siguientes pasos:

1. Ingresar al menú de Windows y seleccionar la opción de Server Manager.

Fig. 84 Paso 1 Procedimiento de Remediación

2. En el menú de Tools ingresar a la opción Computer Management.

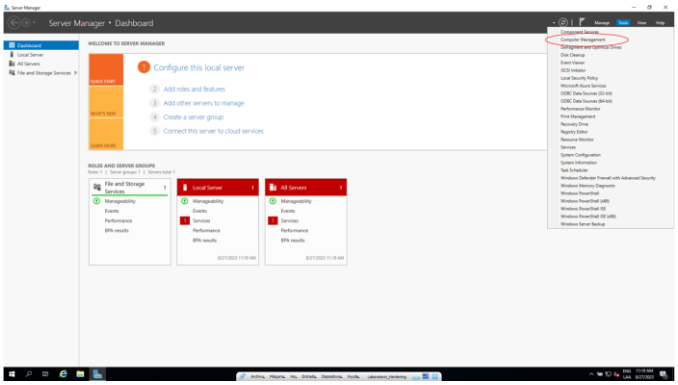

Fig. 85 Paso 2 Procedimiento de Remediación

3. Se debe seleccionar en el menú izquierdo en la opción Local User and Groups la carpeta de Users, esto desplegara los usuarios locales del sistema.

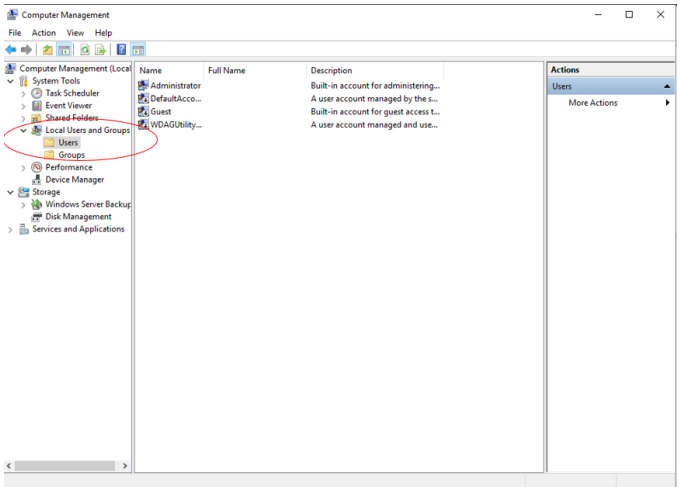

Fig. 86 Paso 3 Procedimiento de Remediación

4. Se procede a renombrar los usuarios Administrator y Guest para lo cual se selecciona cada usuario, con el botón derecho damos click y seleccionamos la opción de Rename

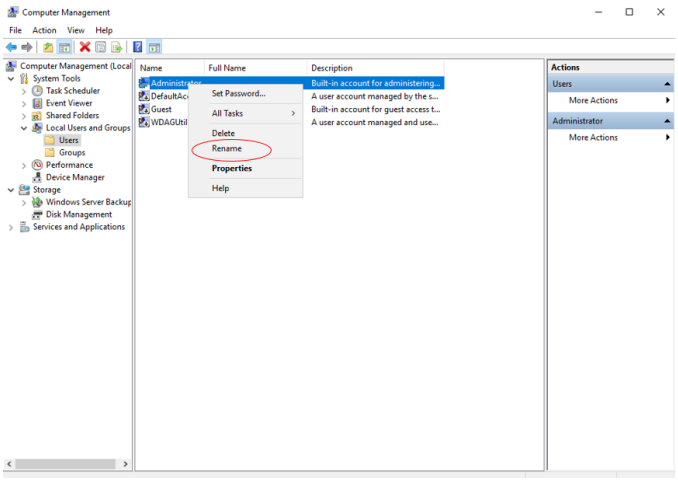

Fig. 87 Paso 4 Procedimiento de Remediación

Se asignará el nombre de principal al Administrator y elotro al usuario Guest.

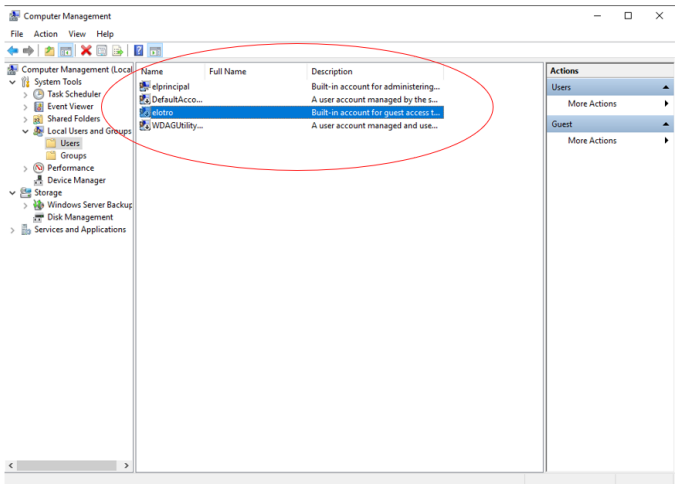

Fig. 88 Asignación de Nombres

Una vez realizada esta actividad se debe reiniciar el sistema y generar nuevamente el reporte AudiTAP para verificar que el cierre de la novedad.

Fig. 89 Remediación Exitosa

Se evidencia que la remediación fu exitosa quedando todas las opciones con cumplimiento.

IX. CONCLUSIONES

- El endurecimiento es una práctica fundamental para protegerse contra las amenazas cibernéticas en un entorno digital cada vez mas hostil.

- La hardenizacion corresponde a una inversion en la proteccion del negocio y de los datos que puede marcar la diferencia entre ser vulnerable a las amenazas o estar preparados para enfrentarlas con mayor confiaza.

- Es necesario contar con conocimientos específicos sobre el sistema a asegurar para llevar a cabo la aplicación de los controles y no generar una indisponibilidad en el servicio.

- El procedimiento de endurecimiento debe ser realizado con periodicidad con el objetivo de permanecer actualizados los controles que mitiguen las nuevas vulnerabilidades

- Existen herramientas gratuitas que se alinean a los benchmark reconocidos en el mercado que facilitan la implementación de los controles

- Siembre deben ser probados los controles en ambientes de pruebas antes de la puesta en producción a fin de minimizar impactos.

X. REFERENCIAS

[1] Cybersecurity Magazine. (2021). CSEC Magazine. Recuperado de: hsecmagazine.com/2021/04/30/hardeninf

[2] NinjaOne. (2022*). Complete Guide to Systems Hardening in 2022*. NinjaOne. Recuperado de: https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening-in-2022/

[3] Centro de Ciberseguridad Industrial (CIS). (2022). *Hardening*. CIS. Recuperado de https://ciset.es/publicaciones/blog/746-hardening

[4] Yacono L. (2023). *System Hardening with DISA STIGs and CIS Benchmarks*. CIMCOR. Recuperado de https://www-cimcor-com.translate.goog/blog/system-hardening-with-disa-stigs-and-cis-benchmarks?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sc#what-are-disa-stigs

[5] Cooper N. (2022). *DISA OKs Automated Benchmark for Microsoft Windows Server 2022 STIG*. ExecutiveBiz. Recuperado de https://executivebiz.com/2022/12/disa-oks-automated-benchmark-for-microsoft-windows-server-2022-stig/

[6] Departamento de Defensa de los Estados Unidos. (2023). Página de descargas de STIGs. Recuperado de https://public.cyber.mil/stigs/downloads/

[7] Centro de Seguridad de la Información (CIS). (2023). Acerca de nosotros. Recuperado de https://www.cisecurity.org/about-us

[8] Centro de Seguridad de la Información (CIS). (2023). CIS Benchmarks. Recuperado de https://www.cisecurity.org/cis-benchmarks

[9] Microsoft. (2023). Microsoft Azure Security Benchmark Overview. Recuperado de https://learn.microsoft.com/en-us/security/benchmark/azure/overview

[10] Center for Internet Security (CIS). (2023). CIS-CAT Lite. Recuperado de https://learn.cisecurity.org/cis-cat-lite

[11] FB-PRO. (2023). Audit Tap Product Information.} Recuperado de https://www.fb-pro.com/audit-tap-product-information/

[12] Axarnet. (2022). *Windows Server: qué es y características Ventajas*. Blog de Axarnet. Recuperado de: https://axarnet.es/blog/windows-server#

[13] Hosting Diario. (2019). Microsoft Windows Server. Hosting Diario. Recuperado de https://hostingdiario.com/windows-server/

[14] El Cegu. (2018) *[Windows Server 2019] – Disponible para Todos!! y Primera Instalación*. El Cegu. Recuperado de https://www.elcegu.com/windows-server-2019-disponible-para-todos-y-primera-instalacion/

[15] KeepCoding. (Año, mes día de publicación). Título del artículo. KeepCoding. Recuperado de https://keepcoding.io/blog/que-es-virtualbox/

[16] Kuex. (s.f). *Cómo instalar VirtualBox: ¿Cuáles son los requisitos?* Kuex. Recuperado de https://kuex.es/como-instalar-virtualbox-cuales-son-los-requisitos/

XI. BIOGRAFÍA

Luis Felipe López Ruiz, Ingeniero de Sistemas graduado de la Fundación Universitaria Los Libertadores en el año 2005, ejerciendo en cargos de dirección, con distintas certificaciones como auditor interno en sistemas de gestión de seguridad de la información (ICONTEC), Gerencia de Proyectos (Politécnico de Colombia), Especialista en integraciones de Sistemas por medio de REST y SOAP, Arquitecto de soluciones, Administrador de bases de datos MySQL y SQL Server, Administrador de Nube Oracle y actualmente realizando la Especialización en Seguridad Informática en la Universidad Piloto de Colombia.