ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE *HARDENING* MEDIANTE LA HERRAMIENTA DE DEVOPS ANSIBLE

IMPLEMENTACIÓN DE *HARDENING*, MEDIANTE ANSIBLE EN UN SISTEMA OPERATIVO DE SERVIDOR MICROSOFT

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR EN REDES Y TELECOMUNICACIONES

DENNY PAOLA PARDO ROBLES

denny.pardo@epn.edu.ec

DIRECTOR: ING. GABRIELA KATHERINE CEVALLOS SALAZAR

gabriela.cevalloss@epn.edu.ec

DMQ, febrero 2024

CERTIFICACIONES

Yo, Denny Paola Pardo Robles declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

Denny Paola Pardo Robles

denny.pardo@epn.edu.ec

dennypola14022602@gmail.com

Certifico que el presente trabajo de integración curricular fue desarrollado por Denny Paola Pardo Robles, bajo mi supervisión.

Gabriela Katherine Cevallos Salazar

gabriela.cevalloss@epn.edu.ec

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

Denny Paola Pardo Robles

CI: 1752528495

DEDICATORIA

Dedico el siguiente trabajo a mi madre Alexandra, la cual ha estado conmigo en cada uno de mis pasos, por ser mi motivo para seguir adelante cada día. También va dedicado para mi tío Jhonny el cual ha sido un apoyo principal durante toda mi vida académica y por ser parte de mi formación.

De igual manera la dedicatoria va para mis hermanos Verónica y Andrés, los cuales han estado para mí en todos los momentos, dándome ese impulso para seguir.

Denny Pardo

AGRADECIMIENTO

Le doy gracias a Dios por todas las experiencias que me ha permitido vivir, por las oportunidades que me ha dado y por siempre bendecirme.

Me gustaría mostrar un agradecimiento especial a mi mamá y también a mis hermanos que han estado presentes en cada una de mis etapas, por enseñarme que siempre se puede a pesar de las dificultades que la vida presente.

A mis amigas Tais y Nicol por la ayuda de me han brindado en todos estos años de amistad.

A todo mi grupo de amigos que hice durante mi tiempo en la universidad, que han sido una parte importante para poder llegar a este punto, por su ayuda y compañía que me han brindado en todo este tiempo. Principalmente a Ivette, Jhon y Kevin, que han estado conmigo para cualquier situación que se ha presentado.

Finalmente agradezco a mi tutora Gabriela por tener la suficiente paciencia para guiarme en el desarrollo de este trabajo y por la enseñanza en las materias que impartió.

Denny Pardo

ÍNDICE DE CONTENIDOS

RESUMEN

El trabajo de titulación consta del proceso para la implementación de *hardening* en un servidor Microsoft, realizado mediante la herramienta Ansible.

En la primera sección se tiene la descripción del proyecto, el objetivo general, objetivos específicos y el marco teórico que contiene la explicación de cada elemento a utilizar.

La segunda sección tiene la metodología, que es un breve resumen de lo que se desarrolló.

La tercera sección se tiene la instalación de una herramienta de escaneo de vulnerabilidades, la cual permite tener un reporte de cómo se encuentra el sistema operativo. Luego se tiene el nodo controlador en el cual se instaló la herramienta de DEVOPS Ansible y la verificación de la versión que está instalada. La conexión entre las máquinas, Winrm y Ansible, ejecutando el comando *ping-pong*. En esta sección igual se realiza y se ejecuta los *playbooks* para la corrección de las vulnerabilidades de los sistemas operativos. Se ejecuta un segundo reporte de vulnerabilidades luego de aplicar las políticas de seguridad. Como última parte de esta sección se hace una comparación de las vulnerabilidades que se corrigieron con las del primer reporte.

La cuarta sección cuenta con conclusiones del tema, con un aprendizaje extra al contenido que ya se tiene. Además, se proporcionan las recomendaciones para ayudar evitar problemas y errores en la implementación de *hardening* mediante Ansible para un servidor Microsoft.

Como última parte se tiene los anexos correspondientes al proyecto.

PALABRAS CLAVE: *Hardening*, *playbook*, Ansible, vulnerabilidades.

ABSTRACT

The present work consists of the process of implementing hardening on a Microsoft server, executed through the Ansible tool.

The first section contains the description of the project, the general objective, the specific objectives, and the theoretical framework that includes an explanation of each element used.

The second section includes the methodology, which is a summary of what was developed.

The third section has the installation of a vulnerability scanning tool, which allows to have a report of the status of the operating system. Then it has the installation of the Ansible tool on the controller node and the verification in the version that is installed. The connection between the machines, Winrm and Ansible, executes the ping-pong command. In this section, playbooks are also performed and executed for the correction of operating system vulnerabilities. A second vulnerability report is executed after applying the security policies. In the last section, a comparison is made of the vulnerabilities that were corrected with those of the first report.

The fourth section contains the conclusions of the topic, with extra learning to the content that is already available. The recommendations help to avoid any mistakes that may occur when implementing hardening using Ansible for a Microsoft server.

The last part embodies the corresponding annexes of the project.

KEYWORDS: *Hardening, playbook, Ansible, vulnerabilities*

1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

El presente proyecto pretende automatizar un proceso de *hardening* en sistemas operativos de servidor, mediante el uso de la herramienta de DevOps Ansible. Ansible permite automatizar tareas de manera remota; con esto se asegura al sistema operativo de servidor, reduciendo significativamente la superficie de ataques; a la vez se garantiza eficiencia, rapidez y fiabilidad, con menos esfuerzo y riesgo de errores humanos.

Se escaneará el sistema operativo de servidor mediante una herramienta de escaneo de configuración y vulnerabilidades, donde se obtendrá un reporte inicial el cual será comparado con un reporte luego de haber aplicado, mediante Ansible, el *hardening* en el sistema operativo de servidor. Este análisis determinará si se ha mejorado la seguridad del sistema operativo de servidor.

1.1 Objetivo general

Implementar *hardening* mediante la herramienta de DevOps Ansible.

1.2 Objetivos específicos

- Identificar las vulnerabilidades en un sistema operativo de servidor sin políticas de seguridad.
- Instalar la herramienta de Ansible en el nodo controlador
- Implementar el *playbook* para aplicar *hardening* al sistema operativo de servidor.
- Implementar el *playbook* para aplicar *hardening* al sistema operativo de servidor.
- Verificar los resultados obtenidos.

1.3 Alcance

En primera instancia se analizan las características y requerimientos de la herramienta Ansible, además se investigarán herramientas de escaneo, de configuración y vulnerabilidades. Partiendo de esto, se instalará un sistema operativo de servidor, sin ninguna política de seguridad; con la herramienta de escaneo se procede a obtener un primer informe de vulnerabilidades.

Luego se crea una máquina virtual para el nodo controlador, donde se instala Ansible y se crea el *playbook* para aplicar *hardening* al sistema operativo de servidor. Con esto se despliega de manera remota las configuraciones necesarias para la implementación

de *hardening*. Se obtiene un nuevo reporte de vulnerabilidades y se observará cuáles parámetros se han solventado.

1.4 Marco Teórico

Windows Server

Windows Server es una plataforma de distribución de servidores de Microsoft. Está desarrollada por algunos lenguajes de programación siendo C++ el principal junto con *Asembler* [1]. La plataforma permite la compilación de infraestructura como de redes, servidores web y aplicaciones, esto conectando al centro de datos un equipo de trabajo específico.

Windows Server hace conexiones entre servidores locales como el servidor de Azure, en estas conexiones añade capas de seguridad y a su vez permite controlar y monitorear lo que son las aplicaciones y la infraestructura. Este sistema es para múltiples usuarios y procesos, por lo cual muchas empresas hacen uso del mismo por sus grandes características [2].

Entre sus características se encuentran que la administración es sencilla de manejar, es flexible y que tiene un sistema de multiusuarios, lo que permite que todos los empleados de una empresa puedan estar conectados al servidor y así compartir archivos. Para contratar este servicio se debe tomar en cuenta la parte de servidor que está diseñado para el desarrollo de tecnologías y también que la empresa maneje una base de datos.

Windows Server al inicio fue creado con la funcionalidad de ser un servidor de archivos, web e impresiones, teniendo así el primer servidor denominado Microsoft el *Windows* 2000 *Server*, este podía soportar hasta cuatro procesadores. Entre las últimas versiones de servidores *Windows* se encuentran:

- ***Windows Server* 2019**: sistema operativo que permite tener un puente entre servidores de Azure y entornos locales. Esto permite que se tenga una mejor seguridad y a su vez se ve reducido el riesgo hacia las empresas, ya que, cuenta con múltiples casas de seguridad en su sistema operativo. Este servidor permite crear aplicaciones en la parte de la nube, teniendo contenedores y microservicios [3].

  Algunas de sus características son que su capacidad de usuarios y dispositivos es ilimitada, lo que permite licenciar hasta 24 núcleos. Tiene una seguridad avanzada, garantizando que los datos y la información este protegida de

cualquier riesgo; como el control de acceso que se basa en roles, permitiendo que la empresa pueda tener un mejor control con respecto al acceso de los usuarios y las aplicaciones que utiliza. También cuenta con buena estabilidad y rendimiento, lo que permite que la compañía, con forme vaya aumentando sus necesidades, el servidor puede ir creciendo, acoplándose a las necesidades de la empresa [4].

- ***Windows* 2022 *Server:*** Sistema operativo de servidor el cual tiene todo para desarrollar cualquier proyecto, teniendo en su sistema las últimas versiones para las actualizaciones [1]. Este sistema operativo se basa en su versión anterior, mejorando la seguridad, administración e integraciones híbridas con el servidor Azure y plataformas de aplicaciones.

  Entre algunas de sus características está la seguridad, combinada con funciones de otras áreas de *Windows Server*, teniendo una seguridad a profundidad para amenazas avanzadas, protegiendo a los servidores actuales. Cuenta con conectividad segura, donde se tiene la parte de transporte que está habilitado el protocolo HTTPS y TLS1.3, los cuales son importantes ya que cifran los datos y se tiene una comunicación segura. También se encuentra el DNS seguro que cifra las consultas mediante el protocolo HTTPS, cuenta con bloqueo de mensajes del servidor [5].

  Este sistema operativo posee *Windows Admin Center,* el cual posee funcionalidades que permiten informar sobre el estado actual del núcleo y habilitar las características que se tiene [5].

Hardening

Hardening o conocido como endurecedor, es el término utilizado para hacer referencia a la mejora de un sistema operativo. Es el proceso de reducir las vulnerabilidades de red o del sistema operativo, pero esto no hace referencia solo a la parte de *software* o *hardware*, se debe de tomar en cuenta que el usuario también puede ser causante de que existan estos errores en el sistema, ya sea por abrir algún archivo o páginas que no cuente con seguridad [6] [7].

Para poder mejorar un sistema operativo o corregir sus vulnerabilidades, se debe conocer cuáles son los errores o amenazas que tiene el sistema, esto facilitará el

proceso para la corrección de estos. Las amenazas más frecuentes que se presentan son:

- Programas malintencionados: El descargar aplicaciones de páginas que no son seguras, abrir enlaces que han llegado por correo electrónico, etc. Son una amenaza para el sistema, ya que, de esta manera las amenazas pueden entrar al sistema y sabotearlo.
- *Exploits*: Este tipo de amenaza es causadas por algún tipo de vulnerabilidad que tengan las aplicaciones, siendo una entrada para los ataques al sistema. Para evitar esto es recomendable actualizar de manera constante las aplicaciones [7].

Herramienta de escaneo

Estas herramientas o aplicaciones permiten realizar una evaluación para ver en qué condiciones se encuentra el sistema operativo, teniendo un análisis de las vulnerabilidades. Detectan si hay brechas, puntos débiles, o cualquier vulnerabilidad que perjudique al sistema o la red. Las herramientas de escaneo utilizan un proceso que permite evaluar al sistema y automatizarlo, agilizando la exploración de brechas de vulnerabilidad.

Existen algunas herramientas para el escaneo de vulnerabilidades, para diferentes sistemas operativos; muchas de ellas muestran las opciones para solventar las vulnerabilidades que tenga el sistema [8].

Tipo de herramientas para el escaneo de vulnerabilidades:

- SCAP *Compliance Checker:* Es una herramienta *open source*. Esta herramienta que permite verificar cumple con las políticas y normas de seguridad establecidas, también analiza el sistema operativo donde verifica si el sistema operativo tiene malas configuraciones, esto en equipos locales o remotos. Cuando se analiza el sistema operativo, esta herramienta da un reporte de las vulnerabilidades existentes, detalla cada uno de los errores y como se puede corregir cada uno de estos [9].
- Nessus: Es un software que permite escanear a todos los sistemas operativos en busca de vulnerabilidades. Cuenta con el dominio que es Nessusd el cual realiza un escaneo de manera objetiva y por otro lado se encuentra el cliente Nessus el cual muestra un informe de todo lo que se encuentre durante el escaneo del sistema operativos. Se lo puede encontrar por interfaz gráfica o se realiza la instalación mediante comandos [10].

- *OpenVas*: Es una herramienta que realiza un escaneo del sistema operativo para la obtención de vulnerabilidades, en la cual se introduce la dirección IP y realizara un análisis de equipo, donde se obtiene como resultado información del equipo el cual fue analizado, los puertos, configuración que está fallando y posibles amenazas que tenga el software del equipo o el servidor [10].

Marcos de referencia

CIS: Centro de Seguridad de internet o también conocido como por sus iniciales CIS son puntos de referencia los cuales ayudan a los profesionales con la seguridad y la administración de la parte de ciberseguridad. Esto fue creado por un grupo de especialistas en seguridad, con el fin de proteger las amenazas que van saliendo. Las empresas implementan CIS para limitar las vulnerabilidades de seguridad en la parte de internet [11].

Con las herramientas de CIS al tener una variedad permite implementar la protección de los sistemas que han sido heredados en contra de riesgos frecuentes y espontáneos. Tienen una adaptación de medidas como la desactivación de puertos que no se encuentren en uso, eliminación de permisos de aplicaciones necesarios y limitación de privilegios de administrador, mejorando así el rendimiento del sistema [11].

Estos puntos de referencias al ser creados por expertos a nivel mundial tienen una aceptación y reconocimiento por parte de los gobiernos, empresas, academias, etc. CIS tiene una aceptación amplia dentro de la parte de las leyes y los estándares de seguridad [11].

NIST: Siendo la abreviación de "*National Institute of Standars and Technology"* es una dependencia del departamento de Comercio de Estados Unidos, el cual ayuda a la parte de los negocios a comprender los riesgos de seguridad que existen, también administra y reduce los riegos en la parte de redes y datos [12].

NIST se puede implementar para las siguientes áreas, para un negocio:

- Identificación: Se realiza una lista de inventario de todos los equipos que tenga la empresa, hasta de las aplicaciones que se utilicen. Se elabora y comparte políticas de seguridad para todos los equipos. La política de seguridad debe cumplir pasos de seguridad para proteger la información y limitar si se tienen daños en el caso de que exista un ataque.

- Protección: Dentro de la protección se debe de tener un control de los usuarios que accedan a la red. Se debe codificar los datos que sean importantes, ya sea que estén almacenados o que se estén transmitiendo. Además, hay que realizar copias de seguridad de toda la información relevante. Implementar un conjunto de medidas de seguridad para la eliminación de archivos, datos electrónicos o de correos.
- Detección: Se debe revisar constantemente si se tienen registrados ingresos a la red y a los equipos por parte de usuarios que no están autorizados. Tomar en cuenta los puertos USB, ya que por este medio se puede robar información.
- Respuesta: Se debe tener un plan en el caso de que existan ataques al sistema, para que los usuarios tengan conocimientos de o qué está pasando y puedan solventarlo.
- Recuperación: Se restauran los equipos y la parte que fue afectada, implementando nuevas políticas de seguridad e informando qué procesos se realizarán pata la recuperación [13].

MITRE ATTQ&CK: ATT&CK son las siglas de *Tactics Techniques and Common Knowledge*, esto es una base de conocimientos el cual tiene matrices las cuales proporcionan información sobre las técnicas de ataques más comunes y ofrece consejos de cómo solventarlos [14] [15].

Tiene una matriz en la cual se muestra las técnicas de ataques conocidas en un formato fácil de comprender, encontrando en la parte superior las tácticas de ataques y en forma de columnas las técnicas de vulnerabilidad. [14].

Los beneficios que se tiene al utilizar MITRE ATT&CK es que identifica áreas donde existen vulnerabilidades. Permite que la comunicación y el trabajo entre diferentes equipos sea fácil, ayudando a tomar decisiones sobre qué medidas de seguridad se deben implementar. Otros de los beneficios que tiene es su inteligencia ante las amenazas, ya que, proporciona una lista de las técnicas que usan los atacantes, siendo a su vez una herramienta la cual permite analizar los equipos. Puede ser utilizado como un evaluador, colocando las políticas de organización que tiene la empresa, teniendo así un resultado de todas las vulnerabilidades que se pueden presentar como una amenaza para la empresa [16].

Ansible

Ansible es una herramienta *open source,* la cual permite automatizar procesos, permitiendo preparar la infraestructura, gestionar, configurar y organizar los sistemas. Los usuarios que utilizan Ansible automatizan la instalación de *software*, tareas diarias, etc. Es una gran herramienta, la cual, al tener varias funcionalidades, ayuda a mejorar la seguridad de los sistemas operativos [17].

Puede funcionar en sistemas de Unix como de *Windows*, es parte de la distribución de Fedora. En las máquinas en las cuales se realiza la ejecución de la automatización es recomendable que se lo realice en Linux, ya que para máquinas que tengan el sistema operativo *Windows*, se deben utilizar aplicaciones complementarias como *Chocolatey*, la cual permite las conexiones remotas para Ansible. También no depende de un agente para realizar un cambio o ejecutar comandos, ese sistema funciona de manera libre, sin la necesidad de un *software* específico. Algunos de sus beneficios son:

- Es accesible la automatización, ya que no se requiere tener mucho conocimiento para utilizar la herramienta.
- No afecta al rendimiento, porque al no utilizar alguna aplicación en específico o un *software*, se puede ejecutar sin ningún problema.
- Garantiza la seguridad, al realizar todo el proceso por una conexión SSH [18].

Playbooks

Es un plano técnico, el cual se ejecuta sin la intervención de un humano, es compatible con varios usuarios y puede ser direccionado para un conjunto de *hosts*. Se envía desde el nodo controlador para que llegue a los nodos clientes; la ejecución se realiza en el orden de las tareas que fueron escritas dentro del *playbook.* Este tipo de archivo tiene una extensión yml o yaml, el cual tiene por lo menos un *play,* este sirve para mejorar el estado inicial de un sistema operativo [17] [18].

2 METODOLOGÍA

Para el presente proyecto de titulación se realizó una investigación experimental, se trabajó con varios sistemas operativos y herramientas de escaneo de vulnerabilidades. Una vez realizada la investigación de los elementos que se utilizarán, se desarrollaron los siguientes puntos.

Primero se realizó el levantamiento de una máquina virtual en Virtual Box que contiene el sistema operativo *Windows Server* 2022, con esta máquina ya creada se buscó una herramienta de escaneo de vulnerabilidades que se acople al sistema operativo que se utilizó. Se instaló la herramienta de escaneo *Scap Compliance Checker* y se procedió a realizar el primer escaneo del sistema operativo, obteniendo el primer reporte de vulnerabilidades.

Como segundo paso se levantó otra máquina virtual, que es el nodo controlador de Ansible. Se instaló la herramienta Ansible y verificó la versión de la herramienta, para la actualización de los archivos, lo cual permite que se tenga la conectividad entre el nodo controlador y el nodo de *Windows Server*.

Teniendo las dos máquinas se realizó la conexión entre las mismas. Para *Windows Server* se instaló y ejecutó un certificado que permite la conexión de Ansible. En el nodo controlador se instaló Testresourse y Winrm, los cuales permiten que se tenga la conexión entre máquinas. Se creó un archivo el cual contiene los *hosts* para la conexión y en otro archivo se realizó el inventario de los *hosts*. Se realizó el "ping-pong" verificando la conexión entre las dos máquinas.

Con la conectividad de los dispositivos se creó los *playbooks*, los cuales contienden las correcciones de algunos errores que se obtuvieron con el primer reporte de vulnerabilidades, aplicando políticas de seguridad del tipo CIS. Teniendo *playbooks* entre estáticos y dinámicos, se ejecutaron cada uno de estos sin tener algún error al momento de la ejecución. Se realizó un segundo escaneo del sistema operativo.

Finalmente se analizan los resultados, en el reporte final aumentó la aprobación del sistema operativo, se revisó que las políticas de seguridad que fueron aplicadas en el *playbook* se ejecutaron de manera correcta y cada una de estas fue solventada.

3 RESULTADOS

En esta parte se incluye el desarrollo de los objetivos que fueron propuestos en un inicio, por lo que se llegó a tener el *hardening* del sistema operativo Windows Server 2022. Al inicio se tiene la instalación de una herramienta de escaneado de vulnerabilidades, en segundo lugar, se procederá a la instalación de la herramienta de Ansible. Los *playbooks son* los que contienen la solución de las vulnerabilidades, los cuales fueron

correctamente ejecutados, se obtuvo un último reporte de vulnerabilidades que detalla la aplicación de las políticas de seguridad.

3.1 Identificación de las vulnerabilidades sin políticas de seguridad

Para empezar con la resolución del proyecto se instaló la herramienta de escaneo SCAP *Compliance Checker* (SCC). Esta herramienta cuenta con versiones para diferentes sistemas operativos de tipo: Linux, *Microsoft Windows, Red Hat Enterprice,* etc.

En la página web https://public.cyber.mil/stigs/scap/ se puede encontrar el instalador para el sistema operativo que se desea realizar el escaneo. Al igual se encuentra un archivo STIG, el cual contiene las políticas de seguridad CIS, que sirven de referencia para la realización de escaneo de vulnerabilidades y la presentación de un reporte detallado de dichas vulnerabilidades.

Primero se descargó el instalador y el archivo el cual contiene las referencias de políticas de seguridad. El instalador se lo ejecuta en modo administrador, se aceptan los términos y condiciones como se observa en la **Figura 3.1**

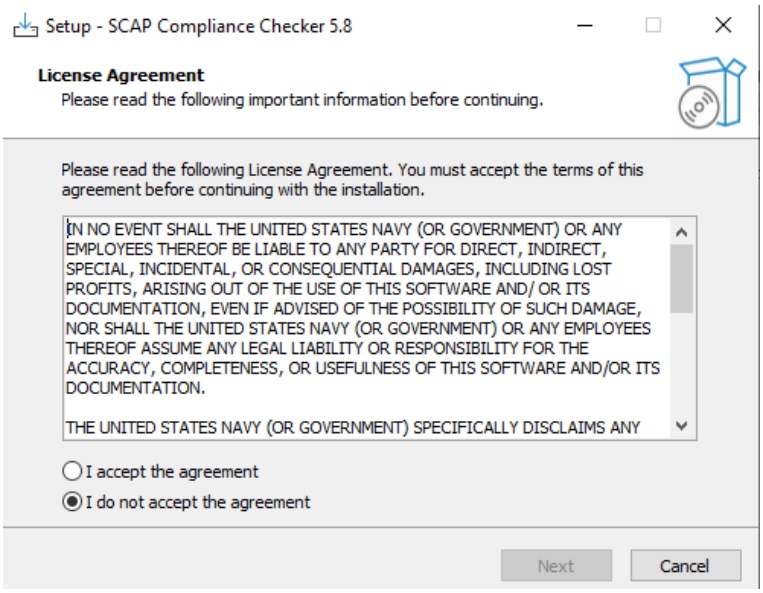


Figura 3.1 Aceptación de términos y condiciones

Se selecciona los casilleros de los complementos que se desean añadir a la instalación como DISA STIG, que es el paquete de políticas de seguridad de diferentes sistemas operativos. En la **Figura *3.2*** puede observar la selección de las instalaciones.

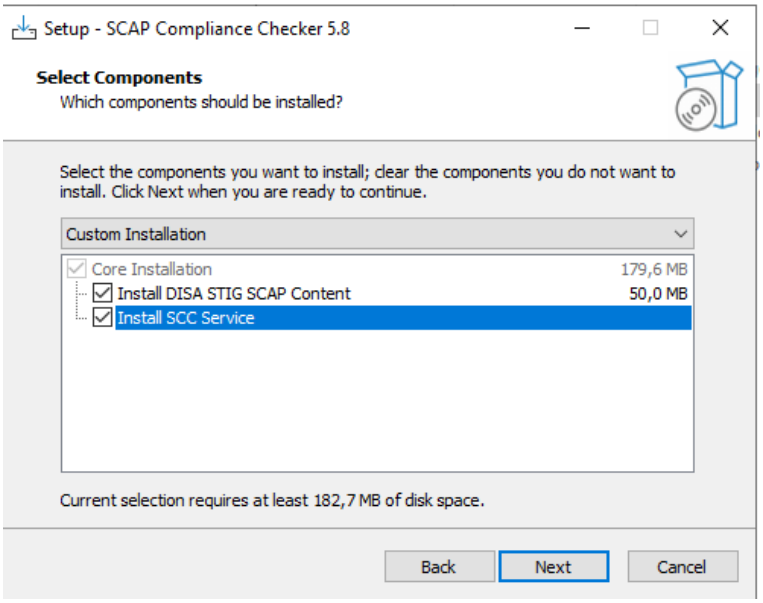


Figura 3.2 Selección de la instalación

Una vez finalizado se inicia la herramienta SCC dentro de la pantalla principal se tienen diferentes opciones, una de ellas es la instalación del archivo que tiene las políticas de seguridad para realizar el escaneo. Como se presenta en la **Figura *3.3***.

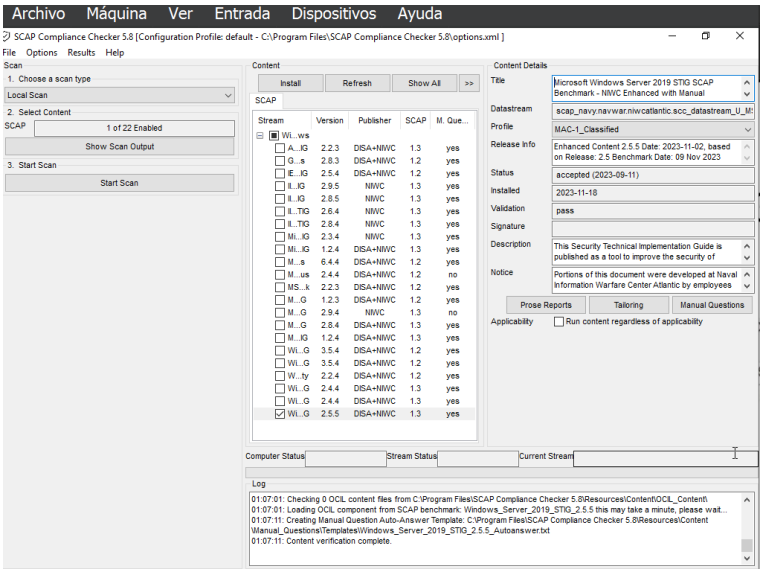


Figura 3.3 Pantalla principal de SCAP

Como siguiente paso se selecciona la versión para la cual se realizará el escaneo, en este caso se escoge la opción para *Windows Server* 2022. Seleccionado el archivo se manda a ejecutar el primer escaneo, mediante el botón de *Start Scan.*

Una vez finalizado el escaneo de las vulnerabilidades se procede a ver el reporte, el cual genera dos archivos: el primero contiene las vulnerabilidades y políticas que

aprobaron el análisis y el segundo archivo solo contiene los errores que presenta el sistema operativo.

El primer reporte presenta un porcentaje de aprobación del sistema operativo del 38.38%, esto se lo puede observar en la **Figura *3.4***.

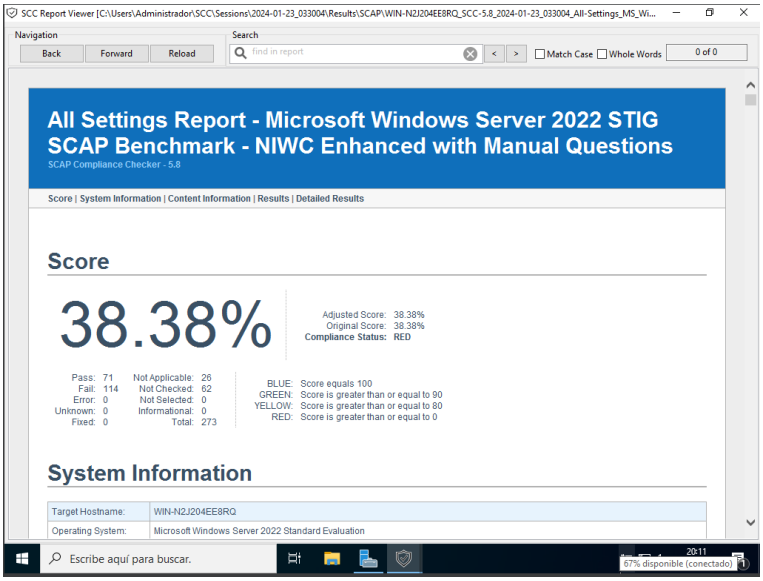


Figura 3.4 Primer reporte

Se evidencian las vulnerabilidades, los ID de cada una y sus correspondientes nombres. Al inicio se tiene la categoría de severidad alta, como se ve en la **Figura *3.5***. Luego se encuentran las de severidad mediana donde se tiene más resultamos, como se evidencia en la Figura 3.6. Por último, se encuentran las de severidad baja, como puede observar en la Figura 3.7.

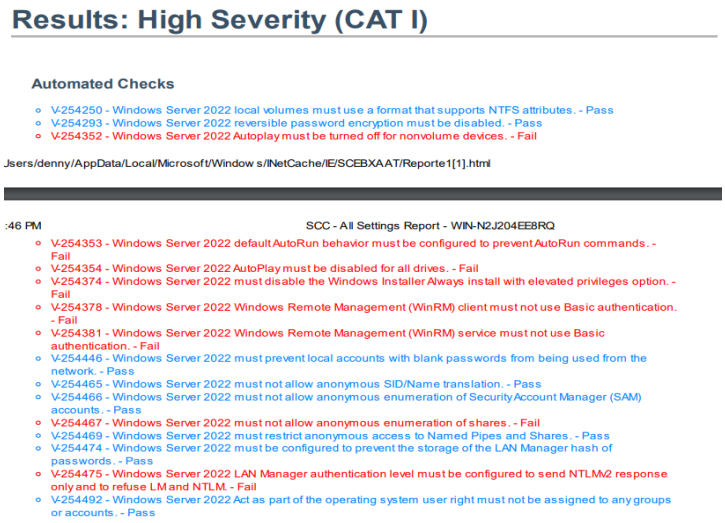
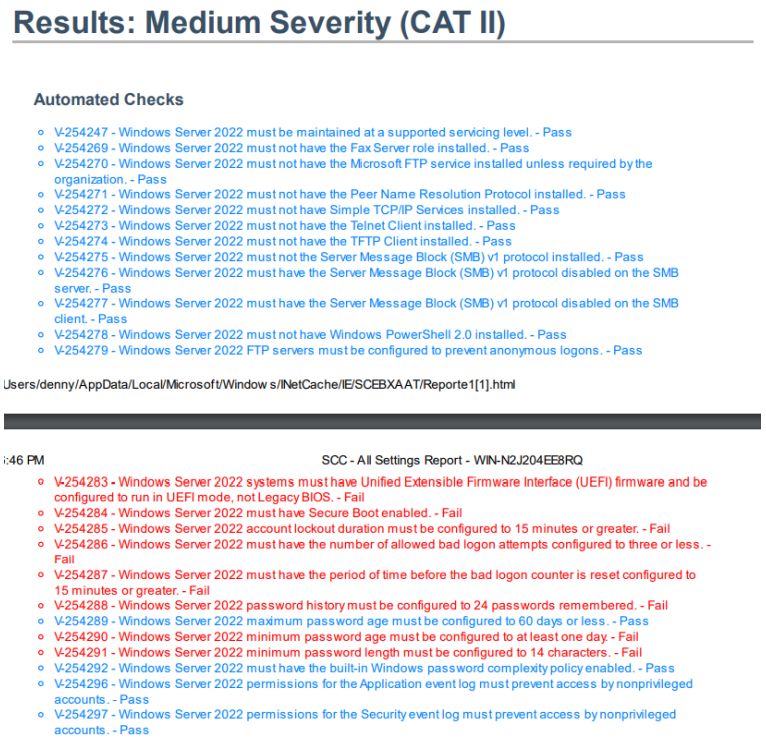


Figura 3.5 Severidad alta



Results: Medium Severity (CAT II)

Automated Checks

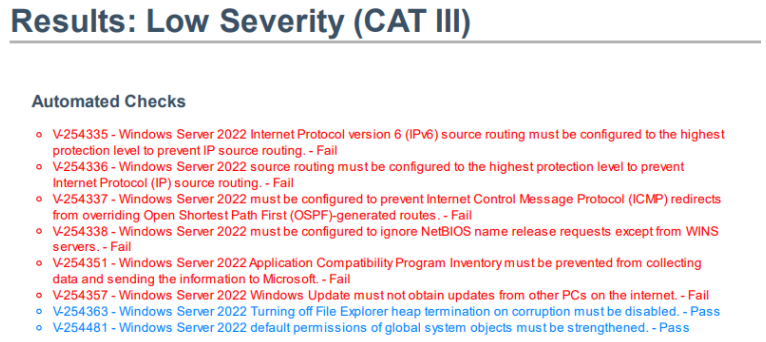
- V-254247 - Windows Server 2022 must be maintained at a supported servicing level. - Pass
- V-254269 - Windows Server 2022 must not have the Fax Server role installed. - Pass
- V-254270 - Windows Server 2022 must not have the Microsoft FTP service installed unless required by the organization. - Pass
- V-254271 - Windows Server 2022 must not have the Peer Name Resolution Protocol installed. - Pass
- V-254272 - Windows Server 2022 must not have Simple TCP/IP Services installed. - Pass
- V-254273 - Windows Server 2022 must not have the Telnet Client installed. - Pass
- V-254274 - Windows Server 2022 must not have the TFTP Client installed. - Pass
- V-254275 - Windows Server 2022 must not the Server Message Block (SMB) v1 protocol installed. - Pass
- V-254276 - Windows Server 2022 must have the Server Message Block (SMB) v1 protocol disabled on the SMB server. - Pass
- V-254277 - Windows Server 2022 must have the Server Message Block (SMB) v1 protocol disabled on the SMB client. - Pass
- V-254278 - Windows Server 2022 must not have Windows PowerShell 2.0 installed. - Pass
- V-254279 - Windows Server 2022 FTP servers must be configured to prevent anonymous logons. - Pass

Users/denny/AppData/Local/Microsoft/Windows/INetCache/IE/SCEBXAAT/Reporte1[1].html

:46 PM SCC - All Settings Report - WIN-N2J204EE8RQ

- V-254283 - Windows Server 2022 systems must have Unified Extensible Firmware Interface (UEFI) firmware and be configured to run in UEFI mode, not Legacy BIOS. - Fail
- V-254284 - Windows Server 2022 must have Secure Boot enabled. - Fail
- V-254285 - Windows Server 2022 account lockout duration must be configured to 15 minutes or greater. - Fail
- V-254286 - Windows Server 2022 must have the number of allowed bad logon attempts configured to three or less. - Fail
- V-254287 - Windows Server 2022 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater. - Fail
- V-254288 - Windows Server 2022 password history must be configured to 24 passwords remembered. - Fail
- V-254289 - Windows Server 2022 maximum password age must be configured to 60 days or less. - Pass
- V-254290 - Windows Server 2022 minimum password age must be configured to at least one day. - Fail
- V-254291 - Windows Server 2022 minimum password length must be configured to 14 characters. - Fail
- V-254292 - Windows Server 2022 must have the built-in Windows password complexity policy enabled. - Pass
- V-254296 - Windows Server 2022 permissions for the Application event log must prevent access by nonprivileged accounts. - Pass
- V-254297 - Windows Server 2022 permissions for the Security event log must prevent access by nonprivileged accounts. - Pass

Figura 3.6 Severidad media



Results: Low Severity (CAT III)

Automated Checks

- V-254335 - Windows Server 2022 Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing. - Fail
- V-254336 - Windows Server 2022 source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing. - Fail
- V-254337 - Windows Server 2022 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes. - Fail
- V-254338 - Windows Server 2022 must be configured to ignore NetBIOS name release requests except from WINS servers. - Fail
- V-254351 - Windows Server 2022 Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft. - Fail
- V-254357 - Windows Server 2022 Windows Update must not obtain updates from other PCs on the internet. - Fail
- V-254363 - Windows Server 2022 Turning off File Explorer heap termination on corruption must be disabled. - Pass
- V-254481 - Windows Server 2022 default permissions of global system objects must be strengthened. - Pass

Figura 3.7 Severidad baja

3.2 Instalación de la herramienta de Ansible en el nodo controlador

Una vez que se obtuvo el primer reporte de vulnerabilidades de *Windows Server* 2022, para la instalación de la herramienta Ansible se levanta una máquina virtual con el sistema operativo Ubuntu 20.4.

Instalación de Ansible

El procedimiento para la instalación de la herramienta Ansible en el entorno de Ubuntu se realiza por medio de un terminal. En primer lugar, se utilizan los comandos ***sudo apt update y sudo apt upgrade*** para la obtención de los repositorios actualizados y descargar todas sus dependencias. Para realizar la instalación de Ansible se emplea el comando ***sudo apt install ansible***, como se puede observar en la Figura **3.8**.

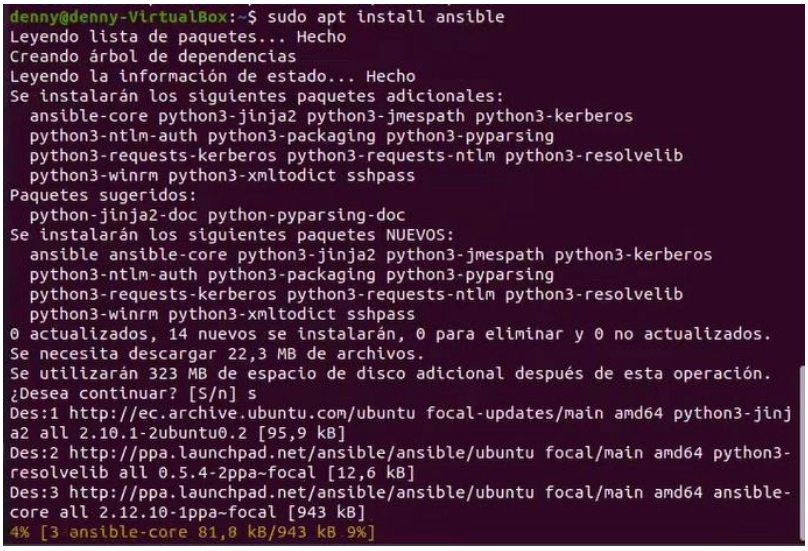


Figura 3.8 Instalación de Ansible

Se debe comprobar que la instalación fue realizada correctamente con el comando ***ansible –version***, el cual verifica que se ha instalado la herramienta y permite observar la versión que se tiene tal y como se muestra en la Figura 3.9.

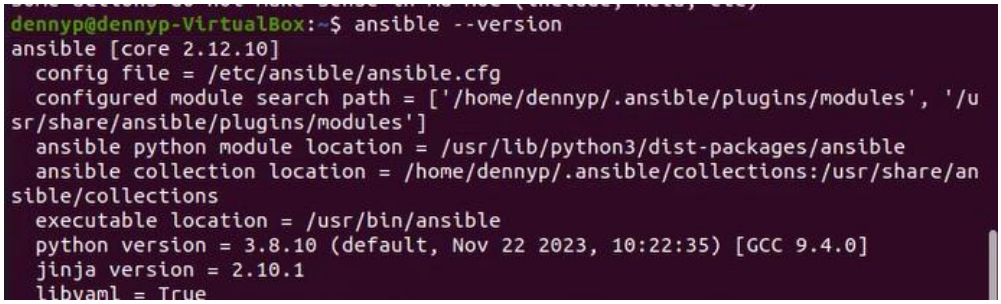


Figura 3.9 Versión de Ansible

3.3 Implementación del *playbook* para aplicar *hardening* al sistema operativo de servidor

Antes de implementar y realizar la ejecución de un *playbook* primero se debe tener conectividad entre el nodo controlador y la máquina que contiene el servidor (nodo controlado). Se toma en cuenta que Ansible realiza las conexiones mediante el protocolo SSH, esto solamente para sistemas operativos UNIX.

Para este caso, debido a que la máquina sobre la cual se realiza el escaneo de vulnerabilidades cuenta con *Windows Server,* el protocolo de conexión entre esta máquina y el nodo controlador se realiza mediante WinRM.

Conectividad entre nodo controlador y el nodo controlado

Empezando con la máquina que tiene *Windows Server* 2022, se descarga un certificado el cual permite la configuración remota para Ansible, dando los permisos necesarios para tener la conectividad.

El certificado que se obtiene es **ConfigureRemotingForAnsible.ps1**. Una vez descargado el archivo se abre la aplicación *Power Shell* y dentro de su consola se accede a la dirección donde fue descargado el certificado, con el comando ***cd: /~Desktop***. Se abre el archivo, tal como se puede apreciar en la Figura 3.10, y se autoriza la ejecución del mismo.

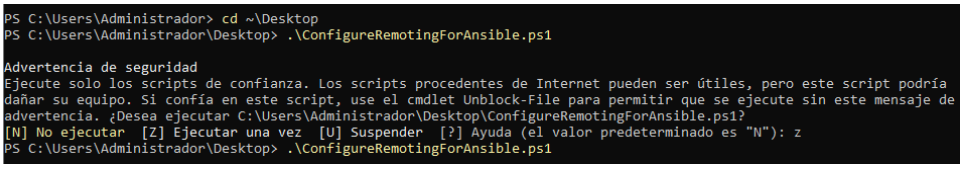


Figura 3.10 Autorización de ejecución

En la máquina del nodo controlador una vez instalado Ansible, y teniendo habilitada la conexión con *Windows Server*, se ejecuta el comando ***sudo python3 -m pip install --user --ignore-installed testresources --no-warn-script-location,*** el cual instala testresources, que es un requisito para poder tener la instalación de pywinrm. Como se puede ver en la Figura 3.11, mediante el uso de este comando se puede acceder a los permisos y archivos necesarios para instalar winrm. Seguido se escribe el comando ***sudo python3 -m pip install --user --ignore-installed pywinrm --no-warn-script-location*** el cual permite tener el acceso a WINRM y que se tenga la conectividad entre las máquinas como se observa en la Figura 3.12 [19].

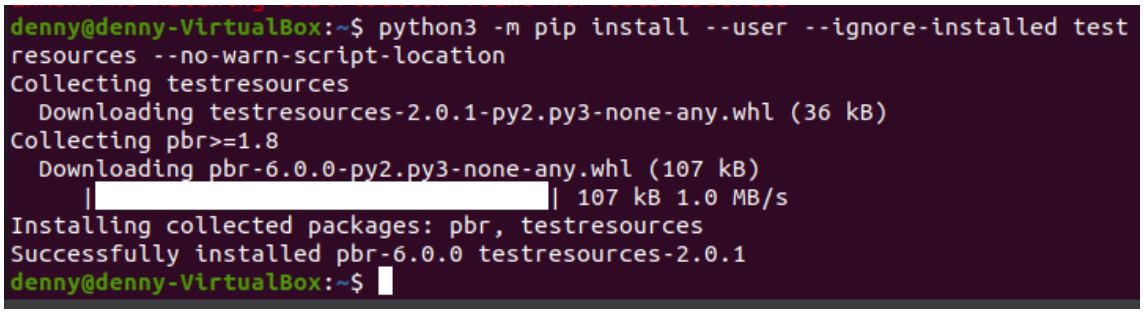


Figura 3.11 Instalación de testrsources

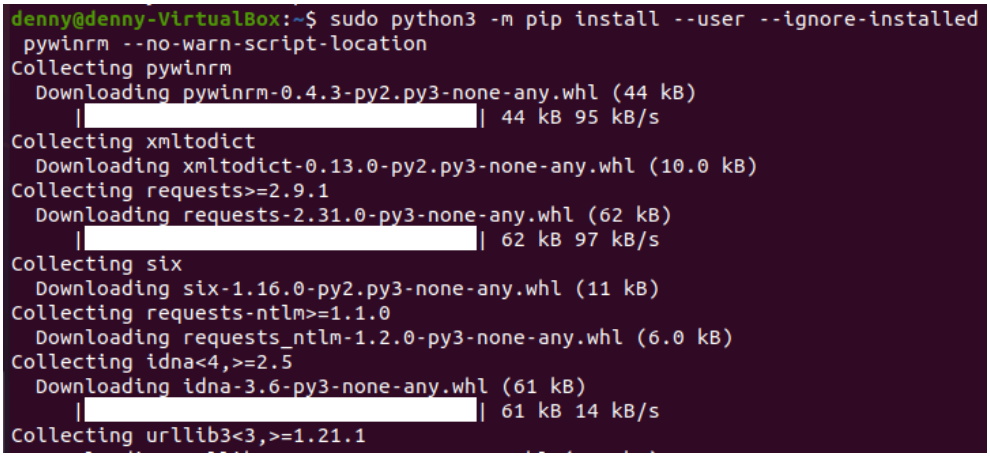


Figura 3.12 Instalación de WinRM

Se creó la carpeta ansible-wind, en la cual se almacenan todos los archivos que son necesario para la conectividad y los *playbooks.* Se ingresa a esta dirección mediante: ***cd ansible-win****.*

Una vez dentro del directorio, como muestra la Figura 3.13, se crea el archivo *host_win* el cual contendrá la lista de los *hosts* a los cuales se le realizó la automatización. En la **Figura *3.14*** se puede ver el contenido del archivo de *host_win*, tomando en cuenta que se debe especificar la dirección IP del *host* al cual se le realizará la corrección de las vulnerabilidades, los usuarios, contraseñas y el puerto por el cual se realiza la conectividad.

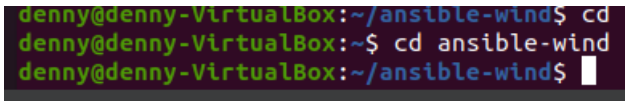


Figura 3.13 Acceso a la carpeta *ansible-wind*

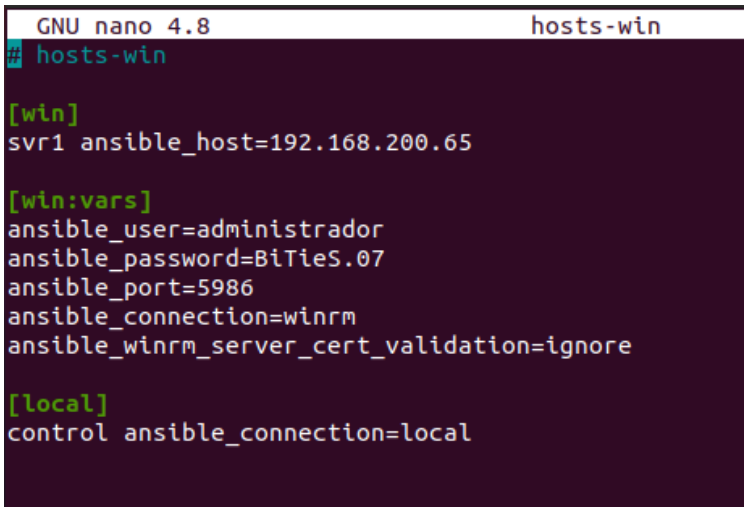


Figura 3.14 Archivos de *hosts*

Se crea el archivo *ansible.cfg*, el cual contiene el inventario de los *hosts*. En este caso, como ya se creó un archivo que contiene la información de los *hosts*, se accede a este

archivo, como muestra la Figura 3.15. Este archivo contiene las llaves y permisos para la conectividad entre las dos máquinas.

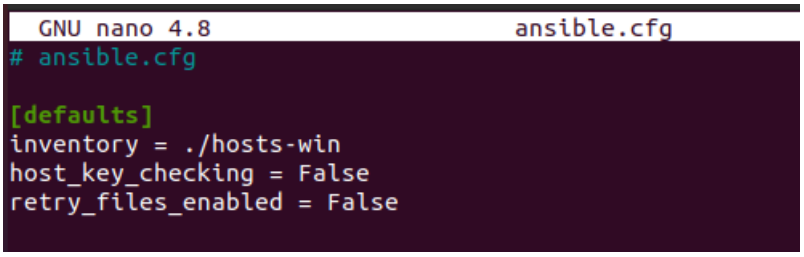


Figura 3.15 Archivo de inventario

Para comprobar la conexión entre las dos máquinas se ejecuta el comando ***ansible -m win_ping svr1*** y cómo se observa en la Figura 3.16 se tiene el ***ping-pong***, el cual da la conectividad de las dos máquinas.

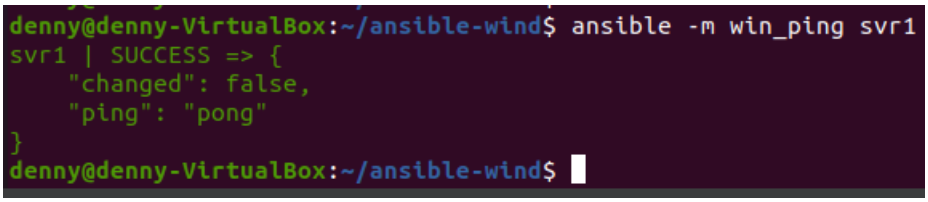


Figura 3.16 Conexión entre máquinas

Creación y ejecución de *playbooks*

Antes de poder aplicar las políticas de seguridad CIS en *Windows Server* 2022, se debe de instalar ***community.windows*** dentro del entorno de Ansible, ya que proporciona unidades de trabajo que Ansible conoce como roles y colecciones***.*** El paquete se lo instala con el comando ***sudo ansible-galaxy collection install community.windows,*** este procedimiento se lo puede ver en la **Figura *3.17***.

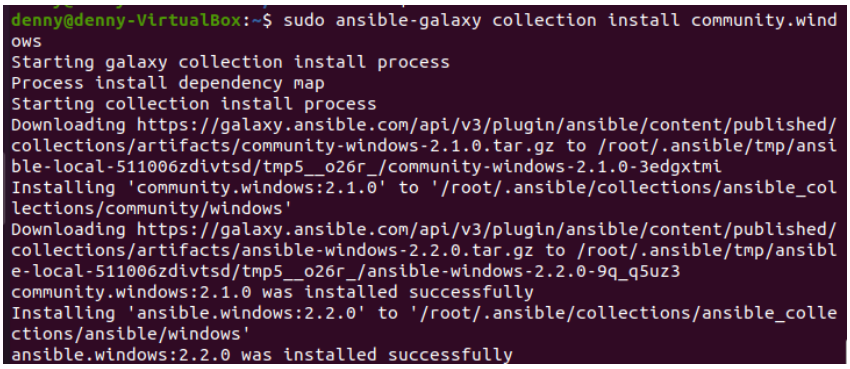


Figura 3.17 Instalación de *Community WIndows*

Con la conexión de las máquinas se procede a crear los *playbooks*, los cuales tendrán las correcciones de algunas vulnerabilidades, las que fueron detectadas en el primer escaneo del sistema operativo. Se creó el primer *playbook* con ***sudo nano playbook_estatico.yml,*** como se ve en la **Figura *3.18.***

```
ws.yaml
denny@denny-VirtualBox:~/ansible-wind$ sudo nano playbook_windows.yaml
```

Figura 3.18 Creación del *playbook* estático

En el contenido del *playbook* estático se puede encontrar el código de cada error a corregir en cada una de las tareas. Este *playbook* contendrá la corrección de 4 vulnerabilidades. La primera tarea corrige el historial de contraseñas de *Windows Server* 2022, se debe configurar para recordar 24 contraseñas. En la **Figura *3.19*** se puede ver aplicada esta política de seguridad.

```
# correccion estaticas
---

- hosts: svr1
  tasks:

    #ERROR V-254288
    - name: Enforce password history' is set to '24 or more password(s)'
      community.windows.win_security_policy:
        section: System Access
        key: PasswordHistorySize
        value: 24
```

Figura 3.19 Corrección ID V-254288

En la segunda tarea se encuentra la solución para la antigüedad mínima de la contraseña de *Windows Server* 2022, lo mínimo en configurarse debe ser un día. En la **Figura *3.20*** se puede ver la solución para esta vulnerabilidad, al igual que el código del error que permite diferenciar cada una de las tareas y qué vulnerabilidad va a solucionar.

```
    #ERROR V-254290
    - name: Ensure 'Minimum password age' is set to '1 or more day(s)'
      community.windows.win_security_policy:
        section: System Access
        key: MinimumPasswordAge
        value: 1
```

Figura 3.20 Corrección ID V-254290

La tarea tres indica la solución para que la extensión mínima de la contraseña de *Windows Server* 2022 se debe configurar en 14 caracteres. Se puede observar en la **Figura *3.21***, que se especifica el valor 14, que es la cantidad mínima de caracteres solicitados para ser aprobada esta condición del sistema operativo.

```
    #ERROR V-254291

    - name: Ensure 'Minimum password length' is set to '14 or more
character(s)'
      community.windows.win_security_policy:
        section: System Access
        key: MinimumPasswordLength
        value: 14
```

Figura 3.21 Corrección ID V-254291

En la cuarta tarea y última del *playbook* estático, esta tarea corrige el nivel de autenticación de *Windows Server* 2022 LAN Manager, se debe configurar para enviar respuesta NTLMv2 para rechazar LM y NTLM. En la **Figura *3.22*** se puede ver la política de seguridad para esta vulnerabilidad.

```
    #Error V-254475
    - name: "Ensure 'Network security: LAN Manager authentication level' is
set to 'Send NTLMv2 response only. Refuse LM & NTLM'"
      win_regedit:
        path: HKLM:\SYSTEM\CurrentControlSet\Control\Lsa
        name: "LmCompatibilityLevel"
        data: "5"
        type: dword
```

Figura 3.22 Corrección ID V-254475

Para realizar los *playbooks* de manera dinámica el formato cambia un poco, como la asignación de las variables de entrada, las cuales se representa con ***vars_prompt***. Esta instrucción se encarga de tomar la respuesta ingresada por el usuario.

El comando ***when*** va en la parte final del *playbook.* Este comando toma la respuesta que fue ingresada por el usuario, si (s) o no (n). Si la repuesta coincide con s la acción se ejecutará. Si es n, esta acción no se realizará.

Se crearon 3 *playbooks* dinámicos diferentes. En la **Figura *3.23***, se puede ver el contenido del primer *palybook*, esta tarea permite corregir la vulnerabilidad de *Windows Server* 2022 Cliente de red de Microsoft: las comunicaciones de firma digital deben estar habilitadas. Para habilitarlo se hace mediante el comando ***data*** donde “1” habilita y “0” deshabilita.

```
---
- hosts: svr1

  vars_prompt:
    #Error V-254460
    - name: pregunta
      prompt: "Desea habilitar s o n "
      private: false

  tasks:


    - name: Habilitar
      win_regedit:
        path: HKLM:-
\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters
        name: RequireSecuritySignature
        data: "1"
        type: dword
      when: pregunta.lower() == 's'
```

Figura 3.23 *Playbook* dinámico 1

En el segundo *playbook* dinámico, la tarea que se ejecutó limita la inactividad de la máquina de *Windows Server* 2022, establecida en 15 minutos o menos, bloqueando el

sistema con el protector de pantalla. En la **Figura *3.24*** se puede ver que se asigna el tiempo en segundos, con el comando ***data.***

```
---
- hosts: svr1

  vars_prompt:

    #Error V-254456
    - name: Iniciomaquina
      prompt: "Desea hacer el inicio de sesión interactivo. Si (s) o No (n) "


  tasks:

    - name: Hacer inicio interactivo
      win_regedit:
        path: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
        name: "InactivityTimeoutSecs"
        data: "900"
        type: dword
      when: Iniciomaquina.lower() == 's'
```

Figura 3.24 *Playbook* dinámico 2

El último *playbook* que se realizó fue el dinámico 3, el cual permite eliminar la tarjeta inteligente de *Windows Server* 2022. Se debe configurar el sistema operativo para forzar el cierre de sesión o bloquear la estación de trabajo. En la **Figura *3.25*** se observa que se habilita esta opción para el cierre de sesión.

```
---
- hosts: svr1

  vars_prompt:

    #Error V-254459
    - name: SmartCard
      prompt: "Desea configurar el cierre forzado de la eliminación de
tarjeta inteligente. Si (s) o No (n) "


  tasks:

    - name: Configuracion cierre forzado de la Tarjeta integrada
      win_regedit:
        path: HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
        name: "ScRemoveOption"
        data: "1"
        type: string
      when: SmartCard.lower() == 's'
```

Figura 3.25 *Playbook* dinámico 3

Con los *playbooks* realizados se procedió a ejecutar cada uno de estos con el comando ***ansible-playbook y el*** nombre *del archivo*. En la **Figura *3.26*** se puede observar que todas las tareas se ejecutaron de manera correcta para los *playbooks* estáticos. En el caso de los *playbooks* dinámicos toma de manera correcta la solicitud ingresada por el usuario, como se puede observar en la **Figura *3.27***.

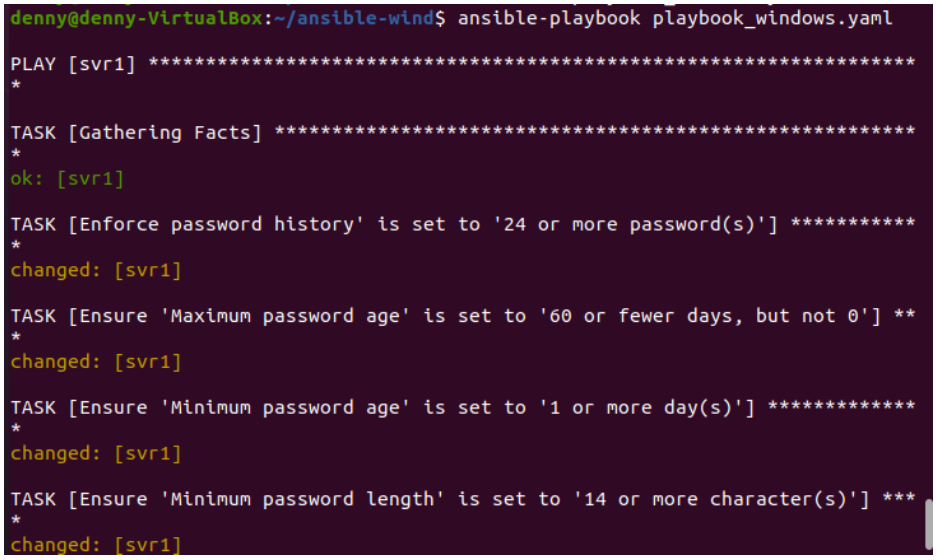


Figura 3.26 Ejecución *playbook* estático

Figura 3.27 Ejecución de un *playbook* dinámico

Segundo escaneo de vulnerabilidades

Con la ejecución de *los playbooks* se realizó un nuevo escaneo de *Windows Server* 2022, para verificar que se hayan corregido los errores y que aumenta la calidad de la seguridad del sistema operativo. Con el segundo reporte de vulnerabilidades obtenido luego de realizar el escaneo, se observa en la **Figura *3.28*** que el porcentaje de aprobación del sistema operativo aumentó, teniendo como resultado final un 42.16% de aprobación.

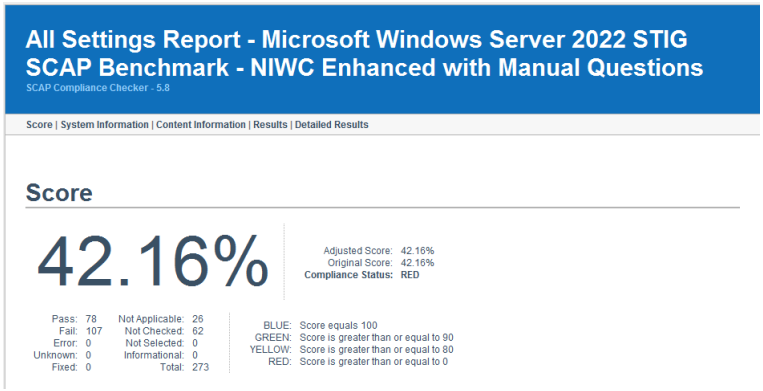


Figura 3.28 Segundo reporte

3.4 Verificación de los resultados obtenidos

Una vez obtenido el segundo reporte de vulnerabilidades y comprobado que se tiene un aumento en la seguridad del sistema operativo *Windows Server*, se puede verificar que los errores elegidos para realizar *hardening* fueron corregidos al 100%.

El primer ID cuyo código es V-254475 pertenece a una vulnerabilidad de categoría alta, como se puede verificar en la **Figura *3.29***, ninguna de las opciones aprobó el test y con el *hardening* se corrigieron todos los errores, como se puede ver en la **Figura *3.30***.

V-254475 - Windows Server 2022 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254475r849241_rule
Test Type:	Automated
Result:	Fail
Version:	WN22-SO-000310
Identities:	CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b)
Description:	The Kerberos v5 authentication protocol is the default for authentication of users who are logging on to domain accounts. NTLM, which is less secure, is retained in later Windows versions for compatibility with clients and servers that are running earlier versions of Windows or applications that still use it. It is also used to authenticate logons to standalone or nondomain-joined computers that are running later versions.
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> Network security: LAN Manager authentication level to "Send NTLMv2 response only. Refuse LM & NTLM".
Severity:	high
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254475 Result: false Title: WN22-SO-000310 - Windows Server 2022 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM. Description: The Kerberos v5 authentication protocol is the default for authentication of users who are logging on to domain accounts. NTLM, which is less secure, is retained in later Windows versions for compatibility with clients and servers that are running earlier versions of Windows or applications that still use it. It is also used to authenticate logons to standalone or nondomain-joined computers that are running later versions. Class: compliance Tests: ◦ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false ('Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Level 5))

Figura 3.29 Código V-254475 con errores

V-254475 - Windows Server 2022 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254475r849241_rule
Test Type:	Automated
Result:	Pass
Version:	WN22-SO-000310
Identities:	CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b)
Description:	The Kerberos v5 authentication protocol is the default for authentication of users who are logging on to domain accounts. NTLM, which is less secure, is retained in later Windows versions for compatibility with clients and servers that are running earlier versions of Windows or applications that still use it. It is also used to authenticate logons to standalone or nondomain-joined computers that are running later versions.
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> Network security: LAN Manager authentication level to "Send NTLMv2 response only. Refuse LM & NTLM".
Severity:	high
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254475 Result: true Title: WN22-SO-000310 - Windows Server 2022 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM. Description: The Kerberos v5 authentication protocol is the default for authentication of users who are logging on to domain accounts. NTLM, which is less secure, is retained in later Windows versions for compatibility with clients and servers that are running earlier versions of Windows or applications that still use it. It is also used to authenticate logons to standalone or nondomain-joined computers that are running later versions. Class: compliance Tests: ○ true (All child checks must be true.) ▪ true (All child checks must be true.) ▪ true ('Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Level 5))

Figura 3.30 Código V-254475 con *hardening*

En el segundo ID cuyo código es V-254288, que pertenece a las vulnerabilidades de mediana categoría, se encarga de almacenar el historial de contraseñas. En la **Figura *3.31*** se puede observar que falla el *test* de aprobación de la vulnerabilidad. La **Figura *3.32*** muestra que el *test está aprobado*.

V-254288 - Windows Server 2022 password history must be configured to 24 passwords remembered.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254288r848680_rule
Test Type:	Automated
Result:	Fail
Version:	WN22-AC-000040
Identities:	CCI-000200 (NIST SP 800-53: IA-5 (1) (e); NIST SP 800-53A: IA-5 (1).1 (v); NIST SP 800-53 Rev 4: IA-5 (1) (e))
Description:	A system is more vulnerable to unauthorized access when system users recycle the same password several times without being required to change to a unique password on a regularly scheduled basis. This enables users to effectively negate the purpose of mandating periodic password changes. The default value is "24" for Windows domain systems. DoD has decided this is the appropriate value for all Windows systems.
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> Enforce password history to "24" passwords remembered.
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254288 Result: false Title: WN22-AC-000040 - Windows Server 2022 password history must be configured to 24 passwords remembered. Description: A system is more vulnerable to unauthorized access when system users recycle the same password several times without being required to change to a unique password on a regularly scheduled basis. This enables users to effectively negate the purpose of mandating periodic password changes. The default value is "24" for Windows domain systems. DoD has decided this is the appropriate value for all Windows systems. Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false ('Enforce password history' is set to '24' passwords or more)

Figura 3.31 Código V-254288 con errores

V-254288 - Windows Server 2022 password history must be configured to 24 passwords remembered.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254288r848680_rule
Test Type:	Automated
Result:	Pass
Version:	WN22-AC-000040
Identities:	CCI-000200 (NIST SP 800-53: IA-5 (1) (e); NIST SP 800-53A: IA-5 (1).1 (v); NIST SP 800-53 Rev 4: IA-5 (1) (e))
Description:	A system is more vulnerable to unauthorized access when system users recycle the same password several times without being required to change to a unique password on a regularly scheduled basis. This enables users to effectively negate the purpose of mandating periodic password changes. The default value is "24" for Windows domain systems. DoD has decided this is the appropriate value for all Windows systems.
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> Enforce password history to "24" passwords remembered.
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254288 Result: true Title: WN22-AC-000040 - Windows Server 2022 password history must be configured to 24 passwords remembered. Description: A system is more vulnerable to unauthorized access when system users recycle the same password several times without being required to change to a unique password on a regularly scheduled basis. This enables users to effectively negate the purpose of mandating periodic password changes. The default value is "24" for Windows domain systems. DoD has decided this is the appropriate value for all Windows systems. Class: compliance Tests: ○ true (All child checks must be true.) ▪ true (All child checks must be true.) ▪ true ('Enforce password history' is set to '24' passwords or more)

Figura 3.32 Código V-254288 con *hardening*

El ID cuyo código es V-254290 igual representa una vulnerabilidad de mediana categoría. No aprobó ninguna de las funciones del *test* como se puede ver en la **Figura *3.33***. Con la aplicación de *hardening* se solventó esta vulnerabilidad, como se ve en la **Figura *3.34***.

V-254290 - Windows Server 2022 minimum password age must be configured to at least one day.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254290r848686_rule
Test Type:	Automated
Result:	Fail
Version:	WN22-AC-000060
Identities:	CCI-000198 (NIST SP 800-53: IA-5 (1) (d); NIST SP 800-53A: IA-5 (1).1 (v); NIST SP 800-53 Rev 4: IA-5 (1) (d))
Description:	Permitting passwords to be changed in immediate succession within the same day allows users to cycle passwords through their history database. This enables users to effectively negate the purpose of mandating periodic password changes.
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> Minimum password age to at least "1" day.
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254290 Result: false Title: WN22-AC-000060 - Windows Server 2022 minimum password age must be configured to at least one day. Description: Permitting passwords to be changed in immediate succession within the same day allows users to cycle passwords through their history database. This enables users to effectively negate the purpose of mandating periodic password changes. Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false ('Minimum Password Age' is set to at least '1' day)

Figura 3.33 Código V-254290 con errores

V-254290 - Windows Server 2022 minimum password age must be configured to at least one day.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254290r848686_rule
Test Type:	Automated
Result:	Pass
Version:	WN22-AC-000060
Identities:	CCI-000198 (NIST SP 800-53: IA-5 (1) (d); NIST SP 800-53A: IA-5 (1).1 (v); NIST SP 800-53 Rev 4: IA-5 (1) (d))
Description:	Permitting passwords to be changed in immediate succession within the same day allows users to cycle passwords through their history database. This enables users to effectively negate the purpose of mandating periodic password changes.
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> Minimum password age to at least "1" day.
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254290 Result: true Title: WN22-AC-000060 - Windows Server 2022 minimum password age must be configured to at least one day. Description: Permitting passwords to be changed in immediate succession within the same day allows users to cycle passwords through their history database. This enables users to effectively negate the purpose of mandating periodic password changes. Class: compliance Tests: ○ true (All child checks must be true.) ▪ true (All child checks must be true.) ▪ true ('Minimum Password Age' is set to at least '1' day)

Figura 3.34 Código V-254290 con *hardening*

El cuarto ID cuyo código es V-254291 pertenece a la categoría de medianas vulnerabilidades. En cada una de las categorías del *test* presenta falla debido a que la contraseña indicada no poseía la longitud mínima establecida, como se ve en la **Figura *3.35***. Con la ejecución del *playbook* se tiene la aprobación de la misma, ver la **Figura *3.36***

V-254291 - Windows Server 2022 minimum password length must be configured to 14 characters.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254291r890539_rule
Test Type:	Automated
Result:	Fail
Version:	WN22-AC-000070
Identities:	CCI-000205 (NIST SP 800-53: IA-5 (1) (a); NIST SP 800-53A: IA-5 (1).1 (i); NIST SP 800-53 Rev 4: IA-5 (1) (a))
Description:	Information systems not protected with strong password schemes (including passwords of minimum length) provide the opportunity for anyone to crack the password, thus gaining access to the system and compromising the device, information, or the local network.
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> "Minimum password length" to "14" characters.
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254291 Result: false Title: WN22-AC-000070 - Windows Server 2022 minimum password length must be configured to 14 characters. Description: Information systems not protected with strong password schemes (including passwords of minimum length) provide the opportunity for anyone to crack the password, thus gaining access to the system and compromising the device, information, or the local network. Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false ('Minimum password length' is set to at least '14' characters)

Figura 3.35 Código V-254291 con errores

V-254291 - Windows Server 2022 minimum password length must be configured to 14 characters.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254291r890539_rule
Test Type:	Automated
Result:	Pass
Version:	WN22-AC-000070
Identities:	CCI-000205 (NIST SP 800-53: IA-5 (1).(a); NIST SP 800-53A: IA-5 (1).1 (i); NIST SP 800-53 Rev 4: IA-5 (1).(a))
Description:	Information systems not protected with strong password schemes (including passwords of minimum length) provide the opportunity for anyone to crack the password, thus gaining access to the system and compromising the device, information, or the local network.
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> "Minimum password length" to "14" characters.
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254291 Result: true Title: WN22-AC-000070 - Windows Server 2022 minimum password length must be configured to 14 characters. Description: Information systems not protected with strong password schemes (including passwords of minimum length) provide the opportunity for anyone to crack the password, thus gaining access to the system and compromising the device, information, or the local network. Class: compliance Tests: ○ true (All child checks must be true.) ▪ true (All child checks must be true.) ▪ true ('Minimum password length' is set to at least '14' characters)

Figura 3.36 Código V-254291 con *hardening*

La quinta vulnerabilidad de categoría media cuyo código es V-254456 pertenece a una vulnerabilidad media. Como se puede observar en la **Figura *3.37***, el tiempo establecido de inactividad antes de pasar al bloqueo de pantalla es mayor a los 15 minutos y con el *hardening* pasó todos los errores, como se ve en la **Figura *3.38***.

V-254456 - Windows Server 2022 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254456r849184_rule
Test Type:	Automated
Result:	Fail
Version:	WN22-SO-000120
Identities:	CCI-000056 (NIST SP 800-53: AC-11 b; NIST SP 800-53A: AC-11.1 (iii); NIST SP 800-53 Rev 4: AC-11 b; NIST SP 800-53 Rev 5: AC-11 b) CCI-000057 (NIST SP 800-53: AC-11 a; NIST SP 800-53A: AC-11.1 (ii); NIST SP 800-53 Rev 4: AC-11 a; NIST SP 800-53 Rev 5: AC-11 a) CCI-000060 (NIST SP 800-53: AC-11 (1); NIST SP 800-53A: AC-11 (1).1; NIST SP 800-53 Rev 4: AC-11 (1); NIST SP 800-53 Rev 5: AC-11 (1))
Description:	Unattended systems are susceptible to unauthorized use and must be locked when unattended. The screen saver must be set at a maximum of 15 minutes and be password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> Interactive logon: Machine inactivity limit to "900" seconds or less, excluding "0" which is effectively disabled.
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254456 Result: false Title: WN22-SO-000120 - Windows Server 2022 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver. Description: Unattended systems are susceptible to unauthorized use and must be locked when unattended. The screen saver must be set at a maximum of 15 minutes and be password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012 Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false (The machine inactivity limit is set to 15 minutes or less)

Figura 3.37 Código V-254456 con errores

V-254455 - Windows Server 2022 must be configured to require a strong session key.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254455r849181_rule
Test Type:	Automated
Result:	Pass
Version:	WN22-SO-000110
Identities:	CCI-002418 (NIST SP 800-53 Rev 4: SC-8; NIST SP 800-53 Rev 5: SC-8) CCI-002421 (NIST SP 800-53 Rev 4: SC-8 (1); NIST SP 800-53 Rev 5: SC-8 (1))
Description:	A computer connecting to a domain controller will establish a secure channel. The secure channel connection may be subject to compromise, such as hijacking or eavesdropping, if strong session keys are not used to establish the connection. Requiring strong session keys enforces 128-bit encryption between systems. Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> Domain member: Require strong (Windows 2000 or Later) session key to "Enabled".
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254455 Result: true Title: WN22-SO-000110 - Windows Server 2022 must be configured to require a strong session key. Description: A computer connecting to a domain controller will establish a secure channel. The secure channel connection may be subject to compromise, such as hijacking or eavesdropping, if strong session keys are not used to establish the connection. Requiring strong session keys enforces 128-bit encryption between systems. Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188 Class: compliance Tests: ○ true (All child checks must be true.) ▪ true (All child checks must be true.) ▪ true ('Domain member: Require strong (Windows 2000 or Later) session key' is set to 'Enabled')

Figura 3.38 Código V-254456 con *hardening*

El sexto ID cuyo código es V-254459 pertenece a una vulnerabilidad media. En la **Figura *3.39*** se puede observar el fallo producido por la eliminación de la tarjeta inteligente. La **Figura *3.40*** se presenta la corrección de la falla.

V-254459 - Windows Server 2022 Smart Card removal option must be configured to Force Logoff or Lock Workstation.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254459r849193_rule
Test Type:	Automated
Result:	Fail
Version:	WN22-SO-000150
Identities:	CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b)
Description:	Unattended systems are susceptible to unauthorized use and must be locked. Configuring a system to lock when a smart card is removed will ensure the system is inaccessible when unattended.
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> Interactive logon: Smart card removal behavior to "Lock Workstation" or "Force Logoff".
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254459 Result: false Title: WN22-SO-000150 - Windows Server 2022 Smart Card removal option must be configured to Force Logoff or Lock Workstation. Description: Unattended systems are susceptible to unauthorized use and must be locked. Configuring a system to lock when a smart card is removed will ensure the system is inaccessible when unattended. Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false ('Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or 'Force Logoff')

Figura 3.39 Código V-254459 con errores

V-254459 - Windows Server 2022 Smart Card removal option must be configured to Force Logoff or Lock Workstation.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254459r849193_rule
Test Type:	Automated
Result:	Pass
Version:	WN22-SO-000150
Identities:	CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b)
Description:	Unattended systems are susceptible to unauthorized use and must be locked. Configuring a system to lock when a smart card is removed will ensure the system is inaccessible when unattended.
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> Interactive logon: Smart card removal behavior to "Lock Workstation" or "Force Logoff".
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254459 Result: true Title: WN22-SO-000150 - Windows Server 2022 Smart Card removal option must be configured to Force Logoff or Lock Workstation. Description: Unattended systems are susceptible to unauthorized use and must be locked. Configuring a system to lock when a smart card is removed will ensure the system is inaccessible when unattended. Class: compliance Tests: ○ true (All child checks must be true.) ▪ true (All child checks must be true.) ▪ true ('Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or 'Force Logoff')

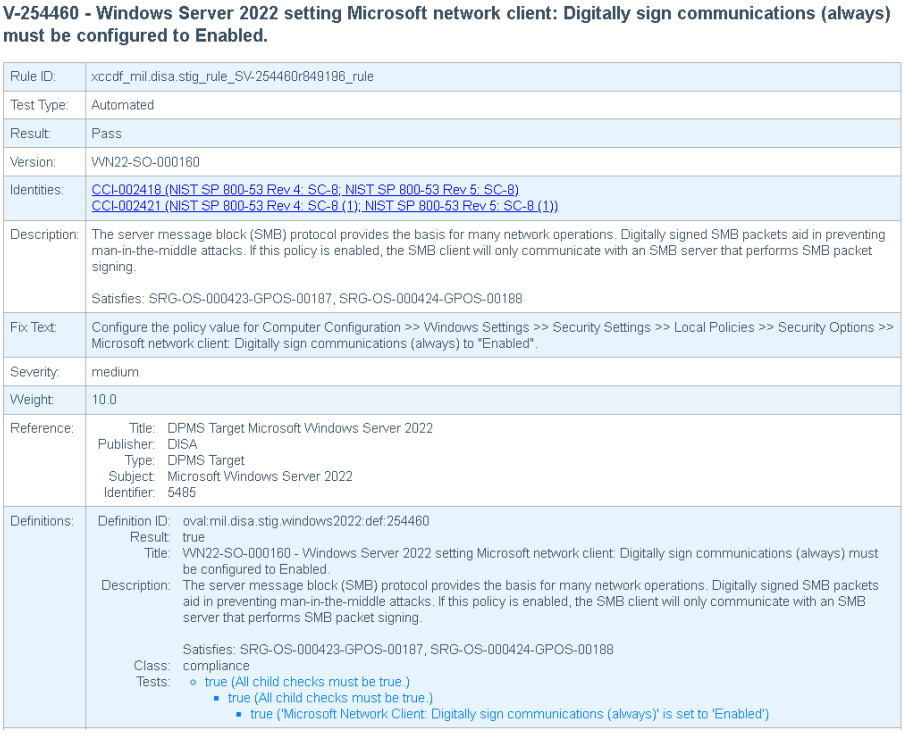
Figura 3.40 Código V-254459 con *hardening*

Como última vulnerabilidad que se tomó para realizar el *hardening* se tiene el ID cuyo código es V-254460, pertenece a una vulnerabilidad media. Presenta los siguientes errores como se puede ver en la **Figura *3.41***, con la ejecución del *playbook* se puede ver en la **Figura *3.42*** que pasa todo el reporte.

V-254460 - Windows Server 2022 setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254460r849196_rule
Test Type:	Automated
Result:	Fail
Version:	WN22-SO-000160
Identities:	CCI-002418 (NIST SP 800-53 Rev 4: SC-8; NIST SP 800-53 Rev 5: SC-8) CCI-002421 (NIST SP 800-53 Rev 4: SC-8 (1); NIST SP 800-53 Rev 5: SC-8 (1))
Description:	The server message block (SMB) protocol provides the basis for many network operations. Digitally signed SMB packets aid in preventing man-in-the-middle attacks. If this policy is enabled, the SMB client will only communicate with an SMB server that performs SMB packet signing. Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> Microsoft network client: Digitally sign communications (always) to "Enabled".
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254460 Result: false Title: WN22-SO-000160 - Windows Server 2022 setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled. Description: The server message block (SMB) protocol provides the basis for many network operations. Digitally signed SMB packets aid in preventing man-in-the-middle attacks. If this policy is enabled, the SMB client will only communicate with an SMB server that performs SMB packet signing. Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188 Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false ('Microsoft Network Client: Digitally sign communications (always)' is set to 'Enabled')

Figura 3.41 Código V-254460 con errores



V-254460 - Windows Server 2022 setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.

Rule ID:	xccdf_mil.disa.stig_rule_SV-254460r849196_rule
Test Type:	Automated
Result:	Pass
Version:	WN22-SO-000160
Identities:	CCI-002418 (NIST SP 800-53 Rev 4: SC-8; NIST SP 800-53 Rev 5: SC-8) CCI-002421 (NIST SP 800-53 Rev 4: SC-8 (1); NIST SP 800-53 Rev 5: SC-8 (1))
Description:	The server message block (SMB) protocol provides the basis for many network operations. Digitally signed SMB packets aid in preventing man-in-the-middle attacks. If this policy is enabled, the SMB client will only communicate with an SMB server that performs SMB packet signing. Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> Microsoft network client: Digitally sign communications (always) to "Enabled".
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2022 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2022 Identifier: 5485
Definitions:	Definition ID: oval:mil.disa.stig.windows2022:def:254460 Result: true Title: WN22-SO-000160 - Windows Server 2022 setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled. Description: The server message block (SMB) protocol provides the basis for many network operations. Digitally signed SMB packets aid in preventing man-in-the-middle attacks. If this policy is enabled, the SMB client will only communicate with an SMB server that performs SMB packet signing. Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188 Class: compliance Tests: ○ true (All child checks must be true.) ▪ true (All child checks must be true.) ▪ true ('Microsoft Network Client: Digitally sign communications (always)' is set to 'Enabled')

Figura 3.42 Código V-254460 con *hardening*

El *hardening* realizado contempla finalmente a 7 vulnerabilidades solventadas, tres de forma dinámica y cuatro de manera estática, todos con una aplicación de las políticas de seguridad de manera correcta, llegando a tener menores vulnerabilidades del sistema *Windows Server* 2022.

4 CONCLUSIONES

- La investigación de varias herramientas de escaneo permitió la obtención de diferentes opciones para el análisis del sistema operativo. Algunas herramientas se encargan de analizar los puertos que están habilitados y no se encuentran enfocados en el análisis de vulnerabilidades de los sistemas operativos como lo son SCAP *Compliance Chacker* y OpenScap.
- No se puede utilizar el sistema operativo sin previamente configurarlo, ya que presenta demasiadas vulnerabilidades que a simple vista no son fáciles de notar. El uso de la herramienta SCAP *Compliance Checker* detalla cada uno de los errores, pero se requiere del archivo STIG que permite tener una guía que ayuda que las políticas de seguridad sean implementadas dentro de los sistemas operativos, el cual es utilizado para realizar pruebas de seguridad informática y comprobaciones de los sistemas operativos.

- La herramienta Ansible es fácil de instalar debido a que solo requiere de un par de comandos; sin embargo, se deben de instalar las diferentes librerías de acuerdo con la automatización que se va a realizar, como en este caso es el *hardening* de un sistema operativo. Se requirió la instalación de *community Windows* que permite tener roles específicos para la automatización de *Windows* mediante los *playbook,* permitiendo aplicar las políticas de seguridad CIS.
- La conectividad entre una máquina que contiene el sistema operativo *Windows Server* y una máquina con sistema operativo Ubuntu se la realiza por el protocolo WinRM y no por SSH, como se lo hace entre distribuciones de UNIX. Para lo cual se requiere obtener el certificado que permite habilitar la configuración remota en *Windows;* con esto se llegan a conectar y establecer comunicación entre la herramienta Ansible instalado en Ubuntu y el sistema operativo de servidor *Windows Serve* 2022.
- Con el certificado de configuración para Ansible, instalado en *Windows Server,* se tiene una comunicación por el puerto 5986 utilizando el protocolo HTTPS, el cual permite que la comunicación esa segura y cifrada para que no pueda ser interceptada.
- Utilizar la herramienta de Ansible permite ahorrar tiempo, ya que los procesos son automáticos y no es necesario la intervención de un técnico, que muchas veces puede cometer errores y así ralentizar el trabajo. Uno de los desafíos al utilizar la herramienta Ansible es escribir de manera correcta los comandos, ya que un error minúsculo impide la ejecución de un *playbook*.
- Se crearon varios *playbooks* dinámicos, debido a que al colocar todas las opciones de petición en un solo *playbook* se genera un error que impide su correcta ejecución. Para cada *playbook* se toma la respuesta del usuario como opción para cada tarea, esto impide el aceptar otra respuesta por cada tarea de manera individual.
- Las tareas dentro del *playbook* estático son más sencillas de implementar, porque estas no requieren de ninguna variable de entrada y se ejecutan todas las tareas, sin que sea necesario que haya interacción con el usuario. Las tareas que contiene el *playbook* estático son definidas con anterioridad y no se pueden modificar durante la ejecución de este.
- Con la obtención del segundo reporte de vulnerabilidades, se comprobó que las políticas de seguridad fueron aplicadas de manera correcta mediante la ejecución de los *playbooks*. En el primer reporte se evidenció que el sistema operativo está seguro en un 38.38%, y en el último reporte se obtuvo un 42.16%;

se corrigieron una vulnerabilidad de alta severidad y seis de media severidad entre tareas dinámicas y estáticas.

- La comparación del primer y el segundo reporte de vulnerabilidades permite verificar si las vulnerabilidades seleccionadas fueron corregidas; observando los códigos de las vulnerabilidades se logra ubicarlas en el nuevo reporte para validar su corrección.

5 RECOMENDACIONES

- Se puede realizar la descarga del certificado, para la configuración de Ansible en *Windows Server* desde el navegador, ya que muchas veces al hacerlo por la consola no se encuentra el archivo.
- Se debería realizar una investigación de cómo conectar de manera remota dos ordenadores, ya que en cada sistema operativo la conexión se lo hace por diferentes protocolos. Esto previo a realizar los *playbooks* que automatizan procesos mediante tareas.
- Para los *playbooks* dinámicos la variable de entrada debería coincidir con la variable reservada, ya que no se guardará la respuesta ingresada por el usuario y no se ejecutará el *playbook*.
- Se puede utilizar un programa de archivos YAML para que verifique que los espacios del archivo creado en Ansible sean correctos, reduciendo errores que puedan existir al momento de la ejecución de un *playbook*.
- Se debería actualizar el sistema operativo del nodo controlador antes de su configuración, para obtener así las últimas versiones de los repositorios. Esto se lo ejecuta mediante los comandos ***sudo apt upgrade*** y ***sudo apt update***, para el sistema operativo Ubuntu.
- Verificar siempre la dirección IP del nodo del Servidor, para que así se mantenga la conectividad entre las máquinas. En este caso en el VirtualBox se empleó una tarjeta de red tipo adaptador puente, lo que permite tener una dirección IP privada y estática.
- En el nodo controlador se debe instalar "*Community Windows",* el cual permite la implementación de las políticas de seguridad CIS para Windows Server 2022 en los *playbooks* que realizan el *hardening*.

6 REFERENCIAS BIBLIOGRÁFICAS

[1] N.A, «axanet,» axarnet, [En línea]. Available: https://axarnet.es/blog/windows-server. [Último acceso: 11 noviembre 2023].

[2] «Microsoft lear,» Microsoft, 30 agosto 2023. [En línea]. Available: https://learn.microsoft.com/es-es/windows-server/get-started/get-started-with-windows-server. [Último acceso: 11 noviembre 2023].

[3] N/A, «Windows server,» Microsoft, 2023. [En línea]. Available: https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2019. [Último acceso: 18 noviembre 2023].

[4] M. A. Cascarano, «Las ventajas de Windows Server 2019 Standard,» Licendi, 22 junio 2023. [En línea]. Available: com/es/blog/las-ventajas-de-windows-. [Último acceso: 18 noviembre 2023].

[5] «Microsoft Learn,» 26 octubre 2023. [En línea]. Available: https://learn.microsoft.com/es-es/windows-server/get-started/whats-new-in-windows-server-2022. [Último acceso: 20 enero 2024].

[6] CISET, octubre04 2022. [En línea]. Available: https://www.ciset.es/publicaciones/blog/746-hardening. [Último acceso: 18 noviembre 2023].

[7] «Ymant Servicios Informáticos,» YMANT, 11 septiembre 2023. [En línea]. Available: https://www.ymant.com/blog/que-es-hardening/. [Último acceso: 18 noviembre 2023].

[8] «Qué es el escaneo de vulnerabilidades y cómo funciona,» Fortra, 25 julio 2022. [En línea]. Available: https://www.fortra.com/es/blog/escaneo-vulnerabilidades#:~:text=Las%20herramientas%20de%20escaneo%20de%20vulnerabilidades%20utilizan%20un%20proceso%20de,aplicaciones%20web%20antiguas. [Último acceso: 18 noviembre 2023].

[9] H. Herrero, «Bloc Bujarra,» 12 septiembre 2023. [En línea]. Available: https://www.bujarra.com/scap-compliance-checker/. [Último acceso: 03 diciembre 2023].

[10] S. d. Luz, «Redes Zone,» 01 octubre 2023. [En línea]. Available: https://www.redeszone.net/tutoriales/seguridad/mejores-escaner-vulnerabilidades-gratis-hacker/. [Último acceso: 03 diciembre 2023].

[11] «AMAZON,» [En línea]. Available: https://aws.amazon.com/es/what-is/cis-benchmarks/. [Último acceso: 19 noviembre 2023].

[12] «federl Tradel Commission,» [En línea]. Available: https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist. [Último acceso: 19 noviembre 2023].

[13] Comision Federal de Comercio, [En línea]. Available: https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist. [Último acceso: 27 novimbre 2023].

[14] «Ciberseguridad.com,» [En línea]. Available: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/. [Último acceso: 27 noviembre 2023].

[15] P. Spencer, «Connectis,» 2023. [En línea]. Available: https://www.connectis.tech/es/the-top-five-cyber-security-frameworks/. [Último acceso: 27 noviembre 2023].

[16] S. Hernandez, «Goba Suite,» 09 noviembre 2013. [En línea]. Available: https://www.globalsuitesolutions.com/es/que-es-marco-mitre-att-ck/. [Último acceso: 27 noviembre 2023].

[17] «Ansible RedHad,» Redhad, noviembre09 2023. [En línea]. Available: https://www.redhat.com/es/technologies/management/ansible/what-is-ansible. [Último acceso: 18 noviembre 2023].

[18] S. Manjaly, «Qué es Ansible: la herramienta DevOps para automatizar tareas de IT,» Ingate, 24 marzo 2023. [En línea]. Available: https://blog.invgate.com/es/ansible. [Último acceso: 18 noviembre 2023].

[19] M. kerry, «markkerry.github.io,» 10 abril 2022. [En línea]. Available: https://markkerry.github.io/posts/2022/04/windows-cis-with-ansible/#setup-the-windows-host. [Último acceso: 2024 enero 12].

7 ANEXOS

ANEXO I. Certificado de originalidad

ANEXO II. Enlace del video demostrativo de la implementación de *hardening*

ANEXO III. Código de los *playbooks*

ANEXO IV. Código QR de los reportes de vulnerabilidades

ANEXO I: Certificado de Originalidad

CERTIFICADO DE ORIGINALIDAD

Quito, D.M. 19 de febrero de 2024

De mi consideración:

Yo, GABRIELA KATHERINE CEVALLOS SALAZAR, en calidad de Directora del Trabajo de Integración Curricular titulado IMPLEMENTACIÓN DE *HARDENING*, MEDIANTE ANSIBLE EN UN SISTEMA OPERATIVO DE SERVIDOR MICROSOFT asociado al proyecto IMPLEMENTACION DE *HARDENING* MEDIANTE LA HERRAMIENTA DE DEVOPS ANSIBLE elaborado por la estudiante DENNY PAOLA PARDO ROBLES de la carrera en Tecnología Superior en Redes y Telecomunicaciones, certifico que he empleado la herramienta Turnitin para la revisión de originalidad del documento escrito completo, producto del Trabajo de Integración Curricular indicado.

El documento escrito tiene un índice de similitud del 12%.

Es todo cuanto puedo certificar en honor a la verdad, pudiendo el interesado hacer uso del presente documento para los trámites de titulación.

NOTA: Se adjunta el link del informe generado por la herramienta Turnitin.

Turnitin TIC Denny Pardo.pdf

Atentamente,

Gabriela Katherine Cevallos Salazar

Docente

Escuela de Formación de Tecnólogos

ANEXO II: ENLACES DEL VIDEO DEMOSTRATIVO DE LA IMPLEMENTACIÓN DE *HARDENING*

Código QR del Video: https://www.youtube.com/watch?v=zPXMeeGQOT8

Anexo I3.4.I.I Código QR de la implementación y pruebas de funcionamiento

ANEXO III: Códigos de los *playbooks*

Playbook estático

```
# correccion estaticas

---


- hosts: svr1

  tasks:


    #ERROR V-254288

    - name: El historial del password debe de estar configurado para recordar 24 passwords o mas

      community.windows.win_security_policy:

        section: System Access

        key: PasswordHistorySize

        value: 24


    #ERROR V-254290

    - name: La vigencia minima de password debe de esta configurado en uno o mas dias

      community.windows.win_security_policy:

        section: System Access

        key: MinimumPasswordAge

        value: 1


    #ERROR V-254291


    - name: La longitud minima del password debe de ser 14 caracteres

      community.windows.win_security_policy:
```

```
      section: System Access
      key: MinimumPasswordLength
      value: 14

  #Error V-254475
  - name: Seguridad de red nivel de autenticación de LAN Manager
    win_regedit:
      path: HKLM:\SYSTEM\CurrentControlSet\Control\Lsa
      name: "LmCompatibilityLevel"
      data: "5"
      type: dword
```

***Playbook* dinámico 1**

```
---
- hosts: svr1

  vars_prompt:
    #Error V-254460
    - name: FirmaDigital
      prompt: "Desea habilitar la firma digital, ya que, las comunicaciones deben de configurarse siempre en habilitadas. Si (s) o No (n) "
      private: false

  tasks:

    - name: Configurar el cliente de red de Microsoft firmar digitalmente
      win_regedit:
```

```
        path:
HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters
        name: RequireSecuritySignature
        data: "1"
        type: dword
      when: FirmaDigital.lower() == 's'
```

Playbook dinámico 2

```
---
- hosts: svr1

  vars_prompt:

    #Error V-254456
    - name: Iniciomaquina
      prompt: "Desea hacer el inicio de sesión interactivo. Si (s) o No (n) "
     private: false

  tasks:

    - name: Hacer inicio interactivo
      win_regedit:
        path: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
        name: "InactivityTimeoutSecs"
        data: "900"
        type: dword
      when: Iniciomaquina.lower() == 's'
```

Playbook dinámico 3

```
---
- hosts: svr1

  vars_prompt:

    #Error V-254459
    - name: SmartCard
      prompt: "Desea configurar el cierre forzado de la eliminación de tarjeta inteligente. Si (s) o No (n) "
      private: false

  tasks:

    - name: Configuracion cierre forzado de la Tarjeta integrada
      win_regedit:
        path: HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
        name: "ScRemoveOption"
        data: "1"
        type: string
      when: SmartCard.lower() == 's'
```

ANEXO IV: Códigos QR de los Reportes de vulnerabilidades

Anexo 3.4.II Primer reporte de vulnerabilidades

Anexo 3.4.III Segundo reporte de vulnerabilidades