Análisis de ciberseguridad a una infraestructura de red implementada en Microsoft Azure

Cybersecurity analysis on network infrastructure implemented in microsoft azure

Ing. José Carlos Gallego Mina jcgallegom@libertadores.edu.co
Universidad de Córdoba

Ing. David Gregorio Rubio Vizcaya dgrubiov@libertadores.edu.co
Fundación Universitaria Los Libertadores

Ing. Héctor Manuel Herrera Herrera hmherrerah@libertadores.edu.co
Fundación Universitaria Los Libertadores

Resumen

Este documento plasma un análisis de ciberseguridad en una infraestructura de red implementada y expuesta en Microsoft Azure, la cual contara con los componentes necesarios para operar. A través de herramientas y técnicas de hacking ético, se hará una exploración de vulnerabilidades sobre esta red, sus componentes y las configuraciones realizadas.

Con los resultados obtenidos de las pruebas, se establece el nivel de seguridad de la infraestructura cloud evaluada y si esta es aceptable para los estándares de integridad, confidencialidad y disponibilidad de la información.

Esto permitirá a los administradores de plataformas Microsoft Azure tener herramientas, guías y bases de seguridad al momento de implementar y asegurar una infraestructura de red en la nube.

Palabras clave: Ciberseguridad, Infraestructura en la nube, análisis de vulnerabilidades, Hacking ético, Microsoft Azure.

Abstract

This document present a cibersecuity annalissis of a inplemented and exposed network infraestructure over Microsoft Azure, this will have the minimal necesary components to operate. Through ethical hacking tools ands techniques, will be a vulnerabily analissis on this network, their components and configurations made.

With the results obtained from the tests, is established the security level of the evaluated network cloud infraestructure and if this is acceptable for the integrity, confidenciality and availability information.

This will permit to the infrastructure administrators on Microsoft Azure have tools, guides and security basis at the time to implement and ensure a cloud network infraestructure.

Keywords: Cybersecurity, Cloud infrastructure, Vulnerability analysis, Ethical Hacking, Microsoft Azure

1. INTRODUCCIÓN

Para las organizaciones la información ha sido, y es, uno de los activos más importantes, por consiguiente, se ha vuelto relevante tomar medidas necesarias para salvaguardarla de posibles amenazas a las cuales está expuesta y que puedan afectar de manera económica, reputacional y legal. Mientras existan vulnerabilidades y personas que puedan explotarlas con la intensión de exigir dinero u obtener información clasificada, ninguna empresa puede considerarse totalmente segura.

Adicional a lo anterior, existe una tendencia de migrar la información, procesos y servicios a plataformas en la nube como lo son Microsoft Azure o Amazon AWS, entre otras, este hecho puede incrementar la vulnerabilidad de la información expuesta en Internet.

En la actualidad existen herramientas acompañadas de técnicas de hacking ético que permiten identificar vulnerabilidades y brechas de seguridad sobre diferentes aplicaciones, servidores, plataformas digitales, redes locales y redes en la nube.

Objetivo general

Analizar la seguridad en la infraestructura de red implementada en la plataforma Azure mediante herramientas de hacking ético.

Objetivos específicos

- Implementar en Azure una infraestructura de red con los componentes necesarios para operación.

- Identificar mediante herramientas de hacking ético las posibles vulnerabilidades sobre la infraestructura de red implementada.
- Evaluar los resultados obtenidos del análisis de vulnerabilidades para identificar el nivel de seguridad sobre la plataforma en la nube de Microsoft.

Pregunta

¿Qué tan segura puede ser una infraestructura de red implementándola en la nube de Azure?

Alcance

La red a implementar en Azure, y sobre la que se realiza el análisis de vulnerabilidades, tendrá dos sub-redes, una publica que constara de una VPN y una privada que estará constituida por: servidores HTTP Linux, servidor de aplicaciones, Servidor Windows SFTP, Active Directory y base de datos Azure SQL server. Mediante procesos y herramientas Open source de Ethical Hacking se procederá a identificar las posibles fallas de seguridad que este tipo de infraestructura en la nube pueden presentar.

Se realizarán dos tipos de pruebas, una externa y una interna, en las cuales se tratara de ingresar y descubrir las vulnerabilidades de la red y de los servicios expuestos, estas pruebas se efectuaran con aplicaciones de penetración como lo son: NMAP y NESSUS ejecutadas desde Linux.

2. REFERENTES TEORICOS

La computación en la nube (cloud computing) se ha posicionado como una de las tecnologías de Internet más usadas y popularizadas para las organizaciones de hoy en día, el migrar su infraestructura de red, aplicaciones y servicios de computo hacia la nube puede traer ventajas económicas de versatilidad, escalabilidad y facilidad para la administración, en contraste, en una plataforma On-premise los mismos beneficios serían más difíciles y costosos de implementar, sin embargo el tener toda una plataforma de tecnología de la información desplegada en Internet también la expone y la hace más susceptible a riesgos de seguridad y ciberataques (Muñoz-Calderón, 2020).

Existen varios modelos de servicios en la nube (Fuentes, 2014) como lo son:

- ***Cloud Software as a Service (SaaS):*** En el Software de nube como servicio, la capacidad proporcionada al consumidor consiste en utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube.
- ***Cloud Platform as a Service (PaaS):*** En la Plataforma de nube como servicio, la capacidad proporcionada al consumidor es desplegar en la infraestructura de nube

aplicaciones adquiridas o creadas por el consumidor, que fueran creadas utilizando lenguajes y herramientas de programación soportadas por el proveedor.

- ***Cloud Infrastructure as a Service (IaaS):*** En la infraestructura de nube como servicio, la capacidad suministrada al consumidor es abastecerse de procesamiento, almacenamiento, redes y otros recursos computacionales fundamentales de forma que el consumidor pueda desplegar y ejecutar software arbitrario.

Este último modelo, IaaS, es el que se utilizara para hacer la implementación y el análisis de ciberseguridad y hacking Ético de la plataforma Cloud, para este caso, el modelo de responsabilidad compartida especifica la menor carga de responsabilidad sobre quien contrata el servicio en la nube (Evelin Pilar Díaz Rodríguez, 2022).

Para plataformas expuestas en servicios Cloud el riesgo de seguridad es potencialmente mayor al tener los servicios expuestos hacia Internet, lo que implica vulnerabilidad a ciberataques, perdida de información, violación de la privacidad, fallas de la disponibilidad del servicio, entre otros. (Mario Casasola Robles (cloudMIDDLEtrust), 2014).

Los riesgos que implican implementar plataformas en la nube son analizados según (Carrasco, 2014) quien hace un estudio de la externalización de los servicios de computo en la nube, los nuevos retos en seguridad informática que esto involucra, analizan también las ventajas de utilizar estas plataformas de nube publica y sobre todo las desventajas desde el punto de vista de seguridad informática.

Aunque no se abordara el análisis en este documento, se recomienda validar la seguridad informática en aplicaciones e infraestructuras implementadas en plataformas cloud afrontando la temática desde el punto de vista legal y de responsabilidades de las partes como es el de la organización que contrata los servicios en la nube, como el proveedor que presta el servicio (O, 2011).

Por último, en cuanto a la responsabilidad compartida para las pruebas de penetración en la nube se deben tener en cuenta los acuerdos de niveles de servicio y obligaciones de cada parte (cliente y proveedor), en este caso el proveedor de la nube es responsable de la seguridad física, de los centros de datos, mientras quien contrata el servicio es responsable de proteger sus datos y aplicaciones almacenados en entorno de la nube en modelo IaaS (startechup, 2023).

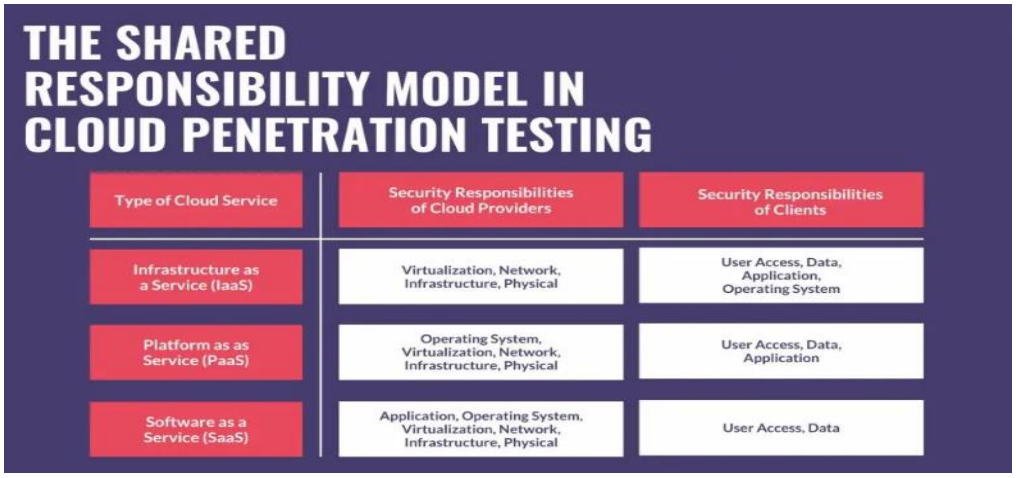


Figura 1. Modelo de responsabilidad compartida en las pruebas de penetración en la nube.
Fuente: Startechup (2023). [Grefico] https://www.startechup.com/es/blog/cloud-penetration-testing/
(startechup, 2023)

Términos y definiciones

- **Azure:** es una gran colección de servidores y hardware de red que ejecutan un conjunto complejo de aplicaciones distribuidas. Estas aplicaciones orquestan la configuración y el funcionamiento del hardware y software virtualizados en esos servidores, esta plataforma es publica y esta implementada en la nube de Microsoft (Microfost, 2023).
- **Cloud Computing (Computación Nube):** Es el uso de una red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software que exponen sus servicios desde internet de manera pública. (Salazar, 2016)
- **Estándar ISO 27017:** proporciona directrices para la implementación de los controles de seguridad de la información en los servicios de la computación en la nube, planeando los escenarios de los clientes y proveedores de este tipo de servicio. Este estándar, se basa en las buenas prácticas de la seguridad de la información definidas en la ISO 27002, y complementa información con respecto a los controles propios de la computación en la nube (BONFANTE, 2019).
- **El estándar ISO 27018** es el primer estándar internacional sobre privacidad en la nube. Esta norma se basa, fundamentalmente, en leyes y regulaciones emitidas en la Unión Europea (Carlos Manual Fernandez, 2015).
- **NMAP:** es una herramienta open source, que permite realizar una serie de escaneos dentro de una red, esta herramienta es multiplataforma, brindando a un administrador de red, a un consultor de seguridad realizar un escaneo acerca de los puertos de red, así como lanzar una serie de scripts para detectar posibles vulnerabilidades en el equipo o red a escanear (Pereda, 2019).
- **NESSUS:** Es una aplicación desarrollada para el escaneo de vulnerabilidad sobre diferentes plataformas o sistemas operativos, posee versiones de código abierto

como de pago y puede ser implementada en sistemas Linux como Windows (tenable, 2023).

Estado del arte

La implementación de infraestructura sobre ambiente cloud permite a las organizaciones tener ventajas sobre infraestructuras On-Premises como menores costos, facilidad de administración, entre otras, sin embargo queda por validar las ventajas de seguridad cuando una infraestructura cloud es implementada para alguna organización (Guevara Jimenez, 2022).

Al igual que la información en ambiente On-premise, en ambientes en la nube esta también es susceptible a ataques como robo, secuestro o daño de la misma , es de aquí donde radica la importancia en la validación de vulnerabilidades que se puedan identificar en estos ambientes, los riesgos expuestos y considerar medidas de aseguramiento del ambiente junto con la información contenida, en este contexto, se han identificado riesgos, sus rangos de criticidad, vulnerabilidades asociadas y la plataforma o nubes relacionadas con varias organización que las tienen contratadas (CUESTAS, 2019).

En la evaluación de seguridad de las principales plataformas en la nube, entre ellas Azure, se presentan razones que descartan a Oracle Cloud o Google Cloud, por motivos de configuración, una interfaz poco amigable lo cual pude hacer que se presenten errores en la configuración abriendo brechas de seguridad de manera involuntaria y que finalmente pueden llegar materializar eventos de seguridad, también falta de claridad en la información legal del servicio a contratar, sobretodo en la nube de Google, en contraste Azure y AWS poseen una plataforma más amigable, contenido para entrenamiento gratuito y tienen claridad con los términos y condiciones y en el ámbito legal acerca del servicio a contratar según la región donde se implemente este (Acevedo, 2022).

Se han realizado informes de seguridad informática donde se realiza un análisis de seguridad de almacenamiento cloud sobre plataforma Microsoft Azure pero estos enfocados a la detección y recuperación de ataques de Ransomware, el impacto de un ataque materializado, los tiempos de recuperación y punto de recuperación, sin embargo no plantea una identificación otras vulnerabilidades a la que pueda estar expuesta esta plataforma (Trevejo, 2022).

Así mismo, existe la descripción de la metodología y especificaciones para realizar pruebas de intrusión en ambientes cloud de AWS con ataques e identificación de vulnerabilidades, usando también, herramientas de hacking ético, aunque en este caso se define la metodología, no se hace un análisis del nivel de seguridad de la plataforma cloud (Pavón, 2022).

Para el proceso de escaneo de vulnerabilidades sobre la plataforma implementada un plan de auditoria puede ser viable como guía metodológica a seguir, identificando las amenazas, riesgos y acciones de mejora asociadas al modelo contratado (IaaS) y los servicios implementados, complementando con una propuesta de remediación. Toda esta evaluación, haciéndola de una manera independiente y objetiva, esto en conjunto permitirá identificar el grado de seguridad del sistema evaluado (Beatriz P. de Gallo1, 2022).

Adicional, se puede implementar una metodología similar que plantea los pasos y procedimientos para ejecutar prueba de penetración sobre aplicaciones móviles sobre nube publica de Google, sin embargo, no expone resultado de la prueba y análisis de los niveles de seguridad detectados, pero parte de la metodología pude ser aplicada para el análisis del presente artículo (Diego Jara, 2017).

3. METODOLOGÍA

Para el desarrollo de este proyecto se va a utilizar una metodología cuantitativa que nos permitirá al final tener datos concretos y confiables para llegar a conclusiones sobre la seguridad en la infraestructura de red en un ambiente cloud sobre Microsoft Azure. En la metodología que se va a usar en el presente estudio, se detallaran los dispositivos que se van a analizar, las técnicas y programas con los cuales se realizaran el análisis de los resultados. Mediante las conclusiones obtenidas en base a los resultados se podrá dar un concepto de que tan segura es una red implementada en la nube de Azure con la infraestructura propuesta (Ver Fig. 2.).

Figura 2. Pasos de la metodología Fuente: elaboración propia

4. RESULTADOS

Implementación de la infraestructura en Azure

En la arquitectura de red implementada los servidores y servicios habilitados corresponden a servicios estándar que normalmente están presentes en las plataformas tecnológicas de cualquier organización, entre estos se incluyen paginas HTTPS, servicios de transferencia de archivos como SFTP y SMB, bases de datos como MSSQL server y MySQL, así mismo se completa con un ambiente conformado con sub-redes y acceso de VPN (Ver Fig. 3.), (Ver Tabla. 1.).

Una de la ventajas al implementar y desplegar la infraestructura en plataforma cloud es la agilidad y versatilidad de la misma, lo cual permitió que el modelo planteado fuera desplegado y configurado en 36 horas aproximadamente, quedando listo para realzar la exploración y el análisis de vulnerabilidades.

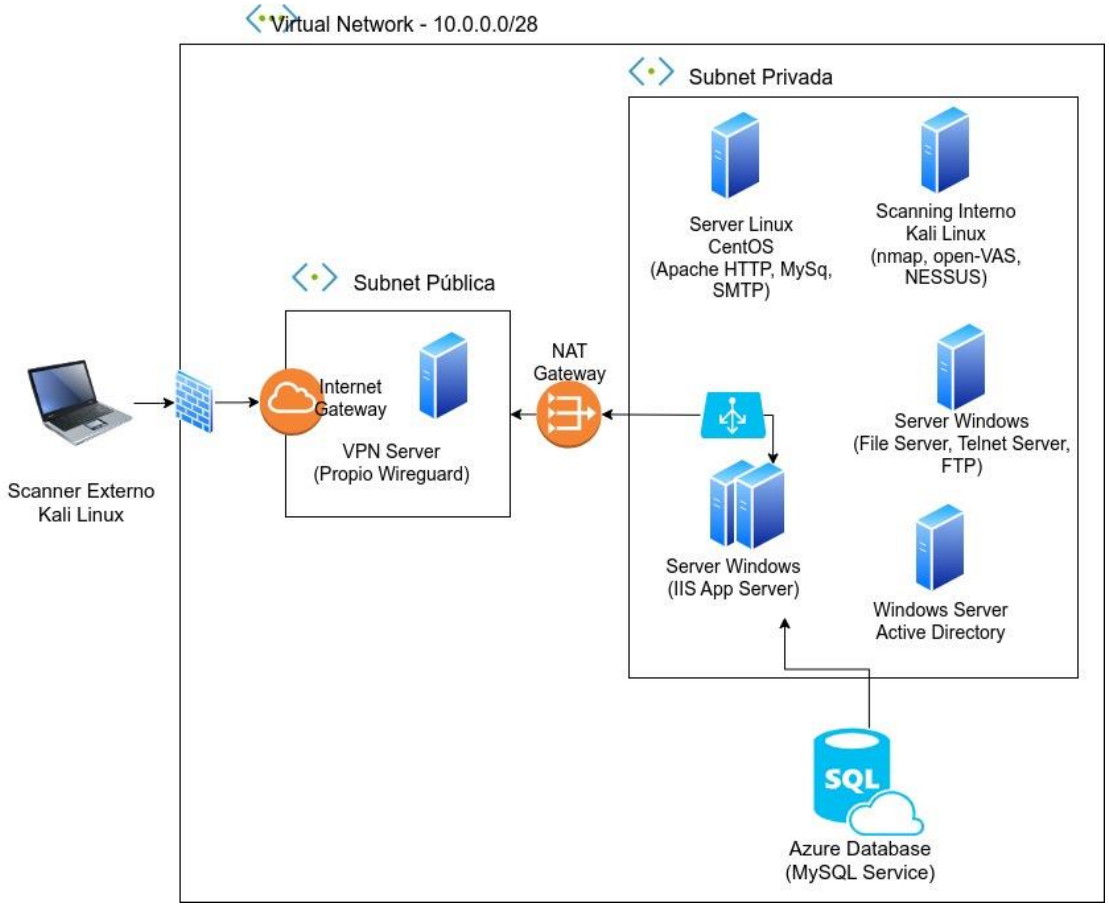


Figura 3. Diseño de la infraestructura de red
Fuente: elaboración propia

Tabla 1. Inventario de la infraestructura implementada

SO	Servicios expuestos o rol	Puertos expuestos	Dirección IP	Red (interna o externa)
Kali Linux	Escáner	N/A	10.0.0.4/28	Interna
CentOS	HTTPS SFTP MYSQL SMTP	TCP 443 TCP 22 TCP 3306 TCP 25	10.0.0.6/28	Interna
Windows Server 2019	Directorio activo (proyect.com.dns)	TCP 3389	10.0.0.5/28	Interna
Windows Server 2016 datacenter	SFTP SMB HTTP RDP	TCP 22 TCP 445 TCP 80 TCP 3389	10.0.0.7/28	Interna
Windows Server 2019	SQL Server RDP	TCP 1433 TCP 3389	10.0.0.8/28	Interna
WINDVPN	Gateway RDP	TCP 3389	10.0.0.20/28	Externa/interna
Azure Virtual Network Gateway	VPN	N/A	N/A	Externa
NAT gateway	N/A	N/A		Interna

Fuente: elaboración propia

Resumen de la implementación

1. Creación de la subscripción en Microsoft Asure
2. Creación de la red virtual
3. Creación de subredes
4. Creación de servidores y máquinas virtuales
5. Creación y configuración de VPN
6. Pruebas de acceso IP publica y VPN

Prueba de instrucción desde maquinas de escaneo interna y externa

Para la ejecución de las pruebas de intrusión se preparan dos máquinas de escaneo Linux para la ejecución de las herramientas NMAP y NESSUS, una de estas máquinas está ubicada fuera de la infraestructura implementada y desde la cual se ejecutara la prueba de

intrusión externo o de caja negra, la otra máquina está ubicada en la red interna de la infraestructura impenetrada en Azure.
En la planeación de las pruebas de intrusión el escaneo de la red completa, se identificaran hosts, puertos abiertos y servicios expuestos así como sus versiones, sistemas operativos, versiones y sobre servicios web identificar carpetas o archivos expuestos.

Ejecución de las pruebas de escaneo

Para el análisis de vulnerabilidades con NMAP y NESSUS se analiza individualmente cada host de la infraestructura y la red completa, con todas las herramientas de escaneo previamente es necesario realizar actualización y descargar de bases de datos de vulnerabilidades. Para la prueba de escaneo externo se analiza la conexión pública que expone la VPN de Azure con la URL (azuregateway-99ba0077-0633-4763-b424-e8197bd83633-9ad228ae9961.vpn.azure.com) o con la IP publica 4.227.194.97. En la prueba Interna el escaneo de vulnerabilidades se direcciona hacia la dirección de red interna del amiente implementado, para este caso es 10.0.0.0/28.

Prueba escaneo externa con NMAP

Comandos usados para el análisis de vulnerabilidades con NMAP en escaneo externo desde Kali Linux, los comandos son parametrizados para generar un archivo de salida en XML (Ver Fig. 4, 5 y 6) para posteriormente convertirlos en formato HTML para su fácil lectura.

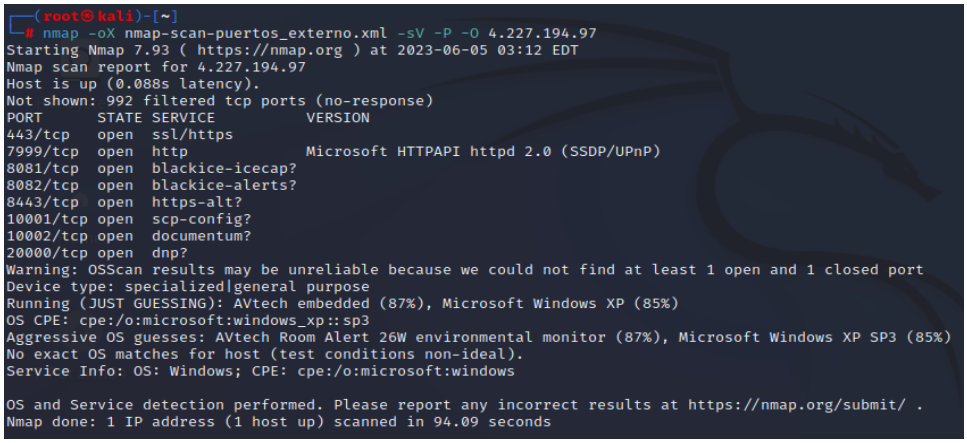


Figura 4. Identificación de puertos, servicios y sistema operativo
Fuente: Elaboración propia

Al realizar el scaner se encontraron varios puertos abiertos, los cuales son el 443, 7999, 8081, 8082, 8443, 10001, 10002, 20000. Estos puertos pueden ser usados para explotar la seguridad los servicio, para poder acceder ilegítimamente a los recursos del servicio, para ingresar al sistema y para poder escalar en privilegios y tomar control del servidor.

Para minimizar la exposición de los puertos que no son necesarios para la conexión VPN se recomienda, en primera instancia tener habilitado y configurado un Firewalll como primera línea de defensa en la red, adicional tener en cuenta las siguientes recomendaciones: Actualizar el firmware de los componentes de red, bloquear protocolo ICMP, realizar escaneos periódicos a la red, usar VLANS para segregación de la red, Implementar IPS (sistema de prevención de intrusos), UTM (Unified Threat Management) y WAF (Web aplication firewall).

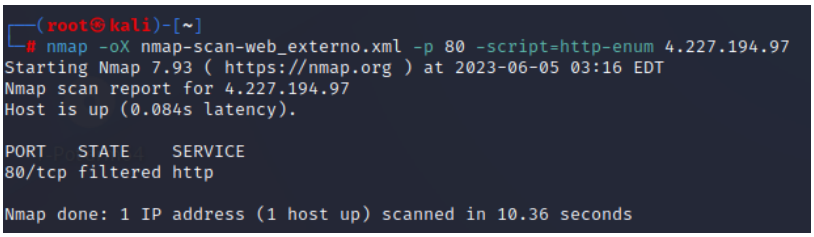


Figura 5. Identificación de archivos o carpetas Web
Fuente: elaboración propia

Para este caso el resultado del scanner no trae ningún tipo de información que algún atacante pueda usar.

Figura 6. Identificar vulnerabilidades con NMAP + Vulscan
Fuente: elaboración propia

Al realizar este análisis se identificaron varios CVE sobre host no asociados a la subscrición, por ejemplo:

- **CVE-2013-3174**: DirectShow en sistemas Windows permite a atacantes remotos ejecutar código arbitrario a través de un archivo GIF manipulado. también conocida como "vulnerabilidad de sobrescritura de memoria arbitraria de DirectShow" (CVE, 2023).

  Mitigación: Esta vulnerabilidad se puede solventar realizando las actualizaciones que Microsoft.

- **CVE-2013-3154**: La funcionalidad de actualización de firmas en Windows Defender en Microsoft Windows 7 y Windows Server 2008 R2 se basa en un nombre de ruta incorrecto, lo que permite a los usuarios locales obtener privilegios a través de una aplicación de caballo de Troya en el directorio de nivel superior %SYSTEMDRIVE%, también conocido como "Microsoft Windows 7 Vulnerabilidad de nombre de ruta inadecuado de Defender" (CVE, 2023).

Mitigación: Microsoft ha sacado actualizaciones para solventar esta vulnerabilidad, se debe actualizar el sistema operativo.

- **CVE-2009-3555**: El protocolo TLS, y el protocolo SSL 3.0 y posiblemente anterior, como se usa en Microsoft Internet Information Services (IIS) 7.0, mod_ssl en Apache HTTP Server 2.2.14 y anterior, OpenSSL anterior a 0.9.8l, GnuTLS 2.8.5 y anterior, Mozilla Network Security Services (NSS) 3.12.4 y versiones anteriores, varios productos de Cisco y otros productos no asocian correctamente los protocolos de enlace de renegociación con una conexión existente, lo que permite a los atacantes intermediarios insertar datos en sesiones HTTPS, y posiblemente otros tipos de sesiones protegidas por TLS o SSL, mediante el envío de una solicitud no autenticada que es procesada retroactivamente por un servidor en un contexto posterior a la renegociación, relacionado con un ataque de "inyección de texto sin formato", también conocido como el problema del "Proyecto Mogul" (CVE, 2023).

  Mitigación: Para actualizar esta vulnerabilidad se debe actualizar el proyecto OpenSSL a la versión más reciente que es 1.0.2 en el momento que se hizo esta documentación.

Prueba escaneo externa con NESSUS

Se ejecuta la aplicación NESSUS a través de navegador web configurando el escaneo externo a la dirección IP pública de acceso a la VPN (Ver Fig. 8.), en el proceso de escaneo externo la aplicación Nessus identifica varias vulnerabilidades (Ver Fig. 9.), estas son catalogándolas por nivel de criticidad. Al finalizar la ejecución de escaneo en Nessus se generan los reportes de vulnerabilidades en formato PDF para ser evaluados.

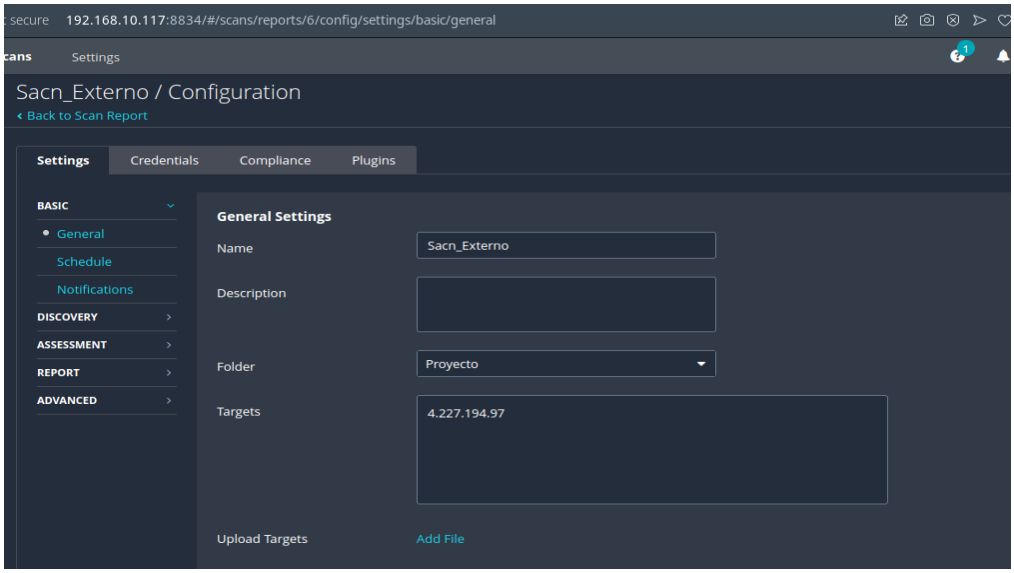


Figura 7. Configuración Nessus escaneo externo Fuente: Elaboración propia

Para poder realizar un análisis de vulnerabilidad con la herramienta Nessus es necesario crear un proyecto en el cual se debe asignar un nombre y una dirección IP o un rango de direcciones IP que se va analizar como objetivo.

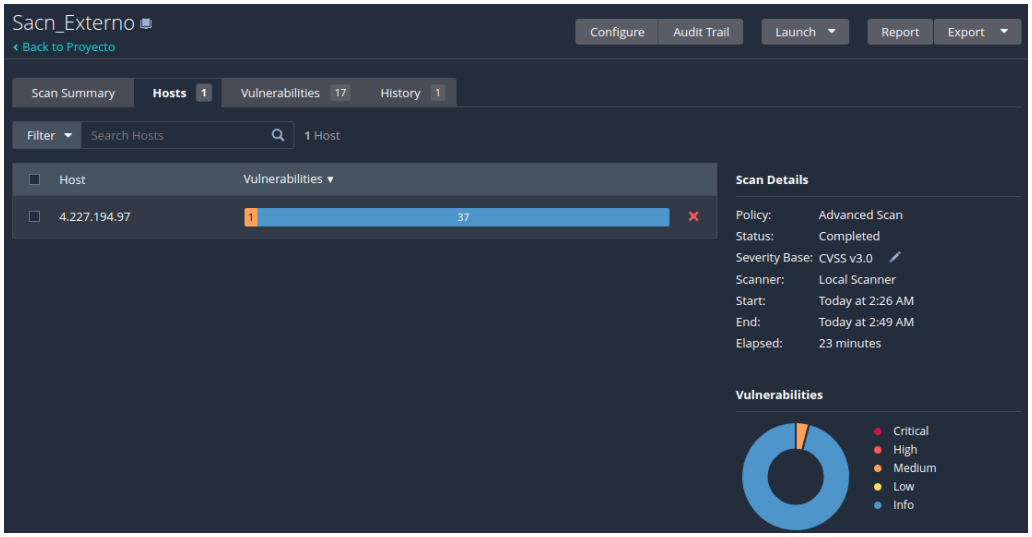


Figura 8. Proceso de escaneo externo con Nessus
Fuente: elaboración propia

El resultado de este análisis de vulnerabilidad encontró que el certificado del servidor no es confiable, este certificado no cuenta con una autoridad certificadora publica conocida, el nivel de criticidad de este hallazgo es Medio y está asociado al ID 51192.

Para solventar esta vulnerabilidad, se puede generar el certificado con una entidad certificadora como lo puede ser GOGETSSL o se puede emitir un certificado SSL con la autenticación del servidor desde la CA emisora de PKI interna y se asigna el certificado en la tienda de RDP y la tienda personal, se elimina el certificado SSL por defecto y el servidor se reinicia.

Otro resulto obtenido fue la identificación de los sistemas operativos de algunas máquinas que están en la infraestructura, el nivel de criticidad de este hallazgo es bajo aunque representa un riesgo ya que identifica la infraestructura o tenant compartido con otros clientes de la plataforma Azure.

Prueba escaneo interna con NMAP

Comandos usados para el análisis de vulnerabilidades con NMAP en escaneo interno desde Kali Linux, al igual que en escaneo externo, los comandos son parametrizados para generar un archivo de salida en XML para posteriormente convertirlos en formato HTML para su fácil lectura (Ver Fig. 9, 10 y 11.).

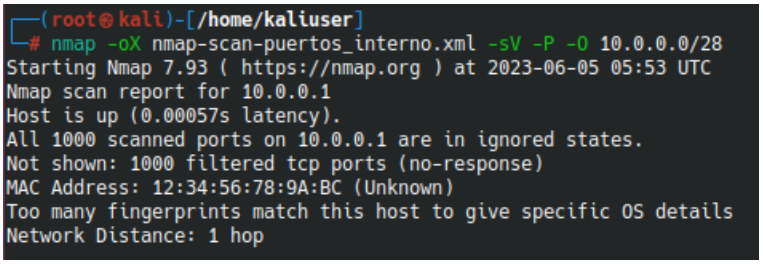


Figura 9. Identificación de puertos, servicios y sistema operativo
Fuente: elaboración propia

Mediante este análisis de vulnerabilidad a la red, no solo se identificó el puerto, si no también información sobre algunos servidores, los puertos encontrados: 22, 53, 80, 88, 135, 139, 389, 443, 445, 3306 4674, 593, 636, 3268, 3269, 3389, 5357. La información que se obtuvo es el sistema operativo y algunos servicios que estos exponen como OPENSSH, MYSQL y APACHE.

La exposición de los puertos puede ser minimizada con tareas de reforzamiento (hardening) del sistema operativo, adicionalmente

Para evitar que puedan conseguir información del Apache se debe modificar el fichero /etc/apache2/conf-available/security.conf se identifican en este archivo las directivas ServerTokens OS y ServerSignature On las cuales se deben modificar y quedar de las siguiente manera ServerTokens Prod y ServerSignature Off, luego de realizar las anteriores modificaciones se procede a guardar los cambios realizados.

Para solventar la vulnerabilidad de OpenSSH se puede editar el archivo que se encuentra en la ruta /etc/ssh/sshd_config y se agrega al final del archivo DebianBanner no, se guardan los cambios y se reinicia el servicio con el comando systemctl restart sshd.

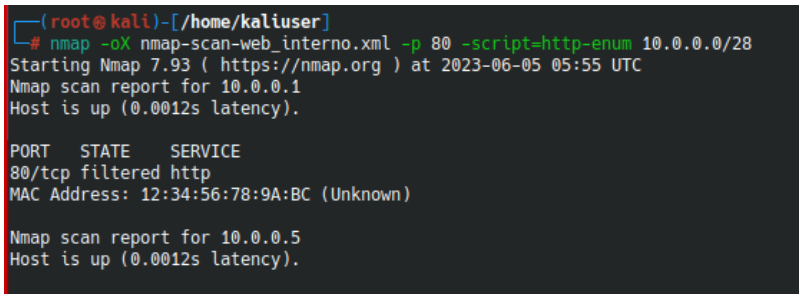


Figura 10. Identificar carpetas o archivos en servidores Web
Fuente: elaboración propia

Al realizar el análisis de puertos en la red interna esta trajo información de algunos puertos e información de un directorio, el puerto expuesto y del que se está adquiriendo la

información de los directorios es el puerto 80 en la IP 10.0.0.6 correspondiente al servidor Linux CentOS de aplicaciones. Esta falla puede ser mitigada aplicado configuraciones correctas sobre el servicio HTTP o en su defecto migra el servicio a HTPPS.

Figura 11. Identificar vulnerabilidades con NMAP + Vulscan
Fuente: elaboración propia

Este análisis trajo varias vulnerabilidades como lo son, por ejemplo:

- **CVE-2006-5229**: OpenSSH portable 4.1 en SUSE Linux, y posiblemente en otras plataformas y versiones, y posiblemente con configuraciones limitadas, permite a atacantes remotos determinar nombres de usuario válidos a través de discrepancias de tiempo en las que las respuestas tardan más para los nombres de usuario válidos que para los no válidos, como lo demuestra sshtime. NOTA: a partir de 20061014, parece que este problema depende del uso de contraseñas configuradas manualmente que causan retrasos al procesar /etc/shadow debido a un mayor número de rondas (CVE, 2023).
  Mitigación: Para esta vulnerabilidad se recomienda la actualización del proyecto OPENSSH

- **CVE-2012-5975** La función SSH USERAUTH CHANGE SOLICITUD en SSH Tectia Server 6.0.4 a 6.0.20, 6.1.0 a 6.1.12, 6.2.0 a 6.2.5 y 6.3.0 a 6.3.2 en UNIX y Linux, cuando La autenticación de contraseña de estilo está habilitada, permite a los atacantes remotos eludir la autenticación a través de una sesión manipulada que involucra la entrada de contraseñas en blanco, como lo demuestra una sesión de inicio de sesión raíz de un cliente OpenSSH modificado con una llamada input_userauth_passwd_changereq agregada en sshconnect2.c (CVE, 2023).
  Mitigación**:** se puede solventar esta vulnerabilidad deshabilitando "old-style" password authentication.

- **CVE-2005-2573**: La función mysql_create_function en sql_udf.cc para MySQL 4.0 anterior a 4.0.25, 4.1 anterior a 4.1.13 y 5.0 anterior a 5.0.7-beta, cuando se ejecuta en Windows, usa una lista negra incompleta en una verificación transversal de directorio, lo que permite a los atacantes incluir archivos arbitrarios a través del carácter de barra invertida (\) (CVE, 2023).
  Mitigación: Esta Vulnerabilidad se solventa con la migración de Mysql a 4.0

Prueba escaneo interna con NESSUS

Se ejecuta la aplicación NESSUS a través de navegador web configurando el escaneo interno a la dirección de red local (Ver Fig. 12,), en el proceso de escaneo interno la aplicación Nessus identifica varias vulnerabilidades por cada uno de los hosts ubicados en la red interna, catalogándolos por nivel de criticidad (Ver Fig. 13.). Al finalizar la ejecución de escaneo en Nessus se generan los reportes de vulnerabilidades en formato PDF para ser evaluados.

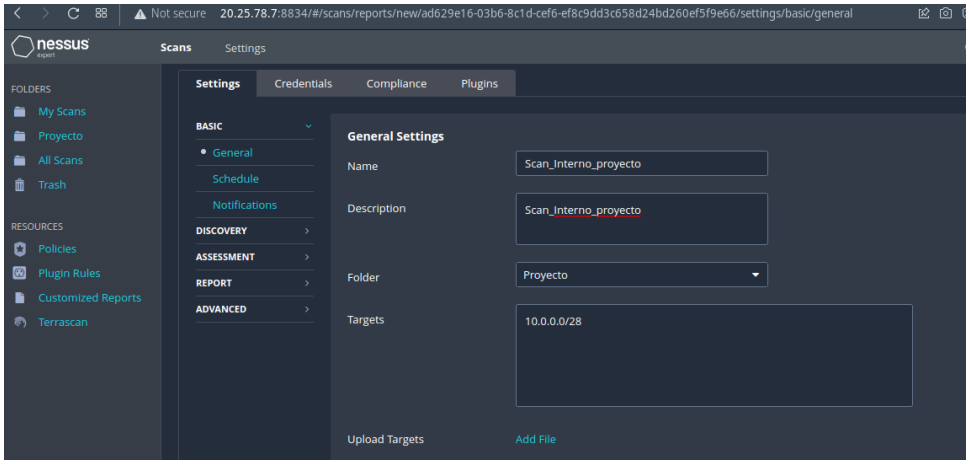


Figura 12. Configuración escaneo interno con Nessus
Fuente: elaboración propia

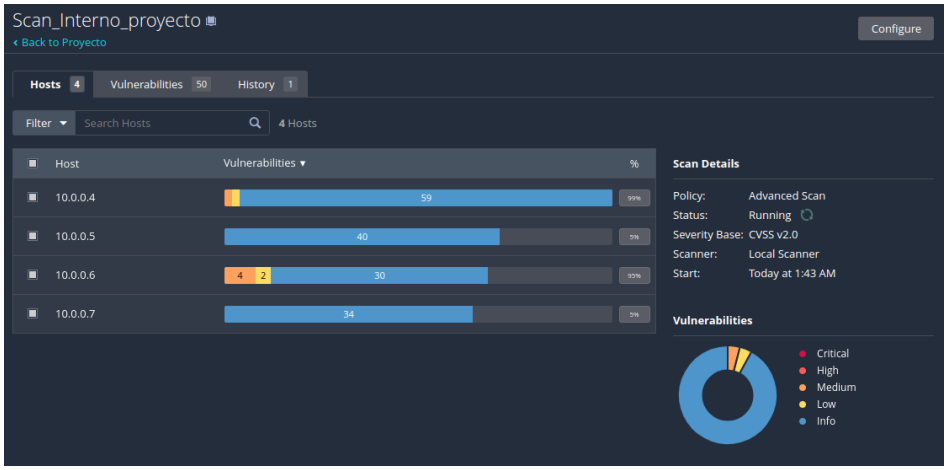


Figura 13. Proceso de escaneo interno con Nessus
Fuente: Elaboración propia

El resultado de este análisis de vulnerabilidad encontró que el certificado del servidor no es confiable, este certificado no cuenta con una autoridad certificadora publica conocida y el nivel de criticidad de este hallazgo es Medio y está asociado al ID 51192.

Otra vulnerabilidad encontrada es que los procesos de demonio en el host remoto están asociados con programas que se han instalado manualmente, este es de prioridad baja y

está asociada al ID 33851. Para mitigarla se debe controlar las herramientas de administración de paquetes nativas de un sistema operativo se utilicen para administrar la instalación, las actualizaciones y la eliminación del software, se debe instalar los paquetes proporcionados por el sistema operativos, preferiblemente que la instalación sea manualmente.

Análisis interno de Microsoft Azure

Automáticamente y a través de Microsoft Defender for Cloud, que es propio de la plataforma Azure, se genera un análisis de seguridad de toda la instancias implementadas en la suscripción, por ejemplo, para el servidor Windows server con rol de directorio activo, dentro la información de falencias de seguridad reportadas se evidencian las siguientes:

Tabla 2. Muestra resultado seguridad de Azure

Recomendación	Descripción	Remediación
Las máquinas virtuales deben cifrar los discos temporales, las cachés y los flujos de datos entre los recursos informáticos y de almacenamiento.	Los discos temporales y las cachés de datos no están encriptados, y los datos no están encriptados cuando fluyen entre recursos informáticos y de almacenamiento. Utilice Azure Disk Encryption para cifrar todos estos datos.	Para habilitar el cifrado de disco en sus máquinas virtuales, siga las instrucciones de cifrado.
El agente de Log Analytics debe instalarse en máquinas virtuales	Defender for Cloud recopila datos de sus máquinas virtuales (VM) de Azure para monitorear vulnerabilidades y amenazas de seguridad. Los datos se recopilan mediante el agente de Log Analytics, que lee varias configuraciones relacionadas con la seguridad y registros de eventos de la máquina para su análisis.	Para conocer varias formas de instalar y configurar su agente de Log Analytics, consulte las instrucciones.

Fuente: elaboración propia

Análisis del resultado de la prueba de instrucción externa o caja negra

El escaneo externo con NMAP no refleja puertos vulnerables expuestos sobre la dirección IP pública de la VPN (Ver Fig. 14.). En relación a carpetas o servicios Web expuesto NMAP no idéntica alguno. Sin embargo en el análisis de NMAP conjunto con VULSCAN a la dirección pública de la VPN se identifican múltiples sistemas expuestos con vulnerabilidades conocidas vulnerables como se evidencia en el reporte generado (Ver Fig. 15.).

Ports

The 992 ports scanned but not shown below are in state: **filtered**

- 992 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
443	tcp	open	https	syn-ack			
7999	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
8081	tcp	open	blackice-icecap	syn-ack			
8082	tcp	open	blackice-alerts	syn-ack			
8443	tcp	open	https-alt	syn-ack			
10001	tcp	open	scp-config	syn-ack			
10002	tcp	open	documentum	syn-ack			
20000	tcp	open	dnp	syn-ack			

Remote Operating System Detection

- Used port: **443/tcp** (**open**)
- OS match: **AVtech Room Alert 26W environmental monitor** (**87%**)
- OS match: **Microsoft Windows XP SP3** (**85%**)

Figura 14. Puertos expuestos VPN
Fuente: elaboración propia

```
MITRE CVE - https://cve.mitre.org:
[CVE-2013-3661] The EPATHOBJ::bFlatten function in win32k.sys in Microsoft Windows XP SP2 and SP3,
[CVE-2013-3660] The EPATHOBJ::pprFlattenRec function in win32k.sys in the kernel-mode drivers in M
[CVE-2013-3174] DirectShow in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows V
[CVE-2013-3173] Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP S
[CVE-2013-3172] Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP S
[CVE-2013-3171] The serialization functionality in Microsoft .NET Framework 2.0 SP2, 3.5, 3.5 SP1,
[CVE-2013-3167] win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows
[CVE-2013-3154] The signature-update functionality in Windows Defender on Microsoft Windows 7 and
[CVE-2013-3138] Integer overflow in the TCP/IP kernel-mode driver in Microsoft Windows Vista SP2,
```

Figura 15. Sistemas detectados sobre la VPN
Fuente: elaboración propia

Como se ve en la anterior, se evidencian multiples sistemas que no están implementados dentro de la infraestructura que se implementó y la suscripción contratada lo cual confirma que Microsof Azure no tiene totalmente independizado los ambientes para diferentes clientes compartiendo un mismo tenant, esto, representando un riesgo en la seguridad del amiente contratado.

En el resultado del análisis externo realizado con Nessus, este solo reporta una vulnerabilidad sobre la IP pública de la VPN en relación al certificado usado para el servicio, el cual es autofirmado (Ver Fig. 16), para la mitigación, este certificado debe ser firmado con una autoridad certificadora oficial.

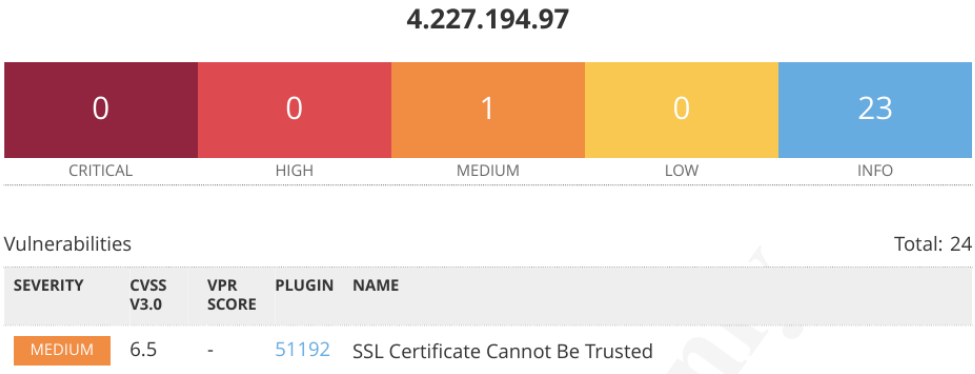


Figura 16. Resultado del análisis externo realizado con Nessus
Fuente: elaboración propia

Análisis de la prueba de instrucción interna o caja blanca

Con NMAP la identificación de puertos, servicios y sistema operativo se envician principalmente para los sistemas Windows la detección de puertos abiertos para los servicios configurados. Por ejemplo, para el servidor de directorio activo se identifican puertos de LDAP, NETBIOS, KERVEROS entre otros, pero adicionalmente se identifican las versiones de los servicios, y para este caso también muestra el nombre de domino y sistema operativo de la maquina como se ve en la siguiente imagen:

10.0.0.5

Address

- 10.0.0.5 (ipv4)
- 12:34:56:78:9A:BC (mac)

Ports

The 987 ports scanned but not shown below are in state: **filtered**

- 987 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack	Simple DNS Plus		
88	tcp	open	kerberos-sec	syn-ack	Microsoft Windows Kerberos		server time: 2023-06-05 05:53:37Z
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
389	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: proyect.com.dns0., Site: Default-First-Site-Name
445	tcp	open	microsoft-ds	syn-ack			
464	tcp	open	kpasswd5	syn-ack			
593	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
636	tcp	open	tcpwrapped	syn-ack			
3268	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: proyect.com.dns0., Site: Default-First-Site-Name
3269	tcp	open	tcpwrapped	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack	Microsoft Terminal Services		
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP

Remote Operating System Detection

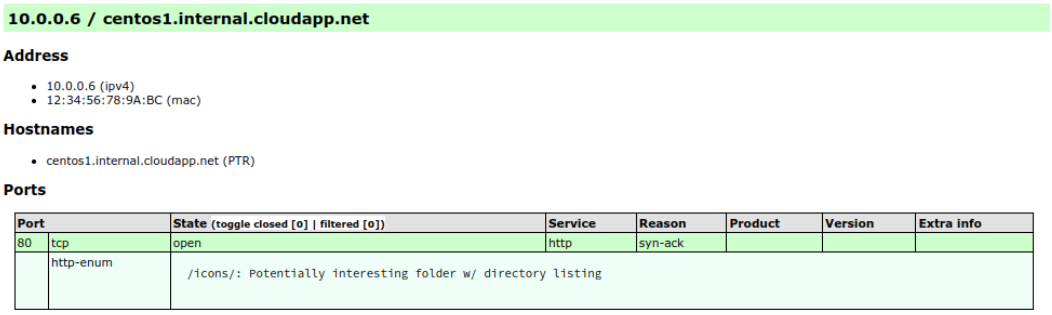
Unable to identify operating system.

- Used port: **53/tcp (open)**

Figura 17. Puertos y versión de servicios sobre servidor Windows
Fuente elaboración propia

Par evitar que un escaneo de puertos esta información sea desplegada se debe realizar un hardening (reforzamiento) de los sistemas operativos, según sea el caso, documentados según recomendación del fabricante.

En la identificación de carpetas o archivos Web para los servidores Linux CentOS y Windows Server de aplicaciones se identificaron los puertos TCP 80 abiertos con exposición de servicio http adicional al configurado HTTPS, puntualmente en el servidor Linux CentOS también identifica carpetas expuestas (Ver Fig. 18).



10.0.0.6 / centos1.internal.cloudapp.net

Address

- 10.0.0.6 (ipv4)
- 12:34:56:78:9A:BC (mac)

Hostnames

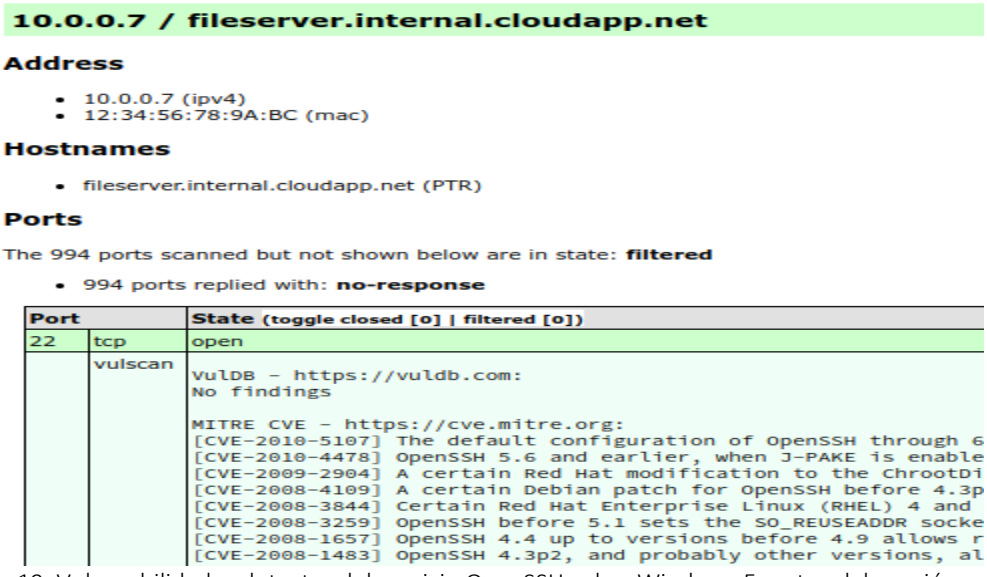
- centos1.internal.cloudapp.net (PTR)

Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack			
	http-enum	/icons/: Potentially interesting folder w/ directory listing					

Figura 18. Carpetas http expuestas sobre Linux CentOS Fuente: elaboración propia

El resultado de la prueba de escaneo de vulnerabilidades con NMAP junto con VULSCAN, arrojo elementos detallados sobre los servicios expuestos en todos los servidores desplegados (Linux y Windows), como ejemplo para el servidor Windows con rol de Fileserver identifico vulnerabilidades asociadas al servicio OpenSSH usado para prestar el servicio SFTP (Ver Fig 19.). De manera similar en el resultado del análisis hecho con Nessus para el mismo servidor reporta 6 vulnerabilidades también relacionadas al servicio SSH asociadas a las versiones del protocolo TLS, y cifrados y algoritmos dediles (Ver Fig. 20.).



10.0.0.7 / fileserver.internal.cloudapp.net

Address

- 10.0.0.7 (ipv4)
- 12:34:56:78:9A:BC (mac)

Hostnames

- fileserver.internal.cloudapp.net (PTR)

Ports

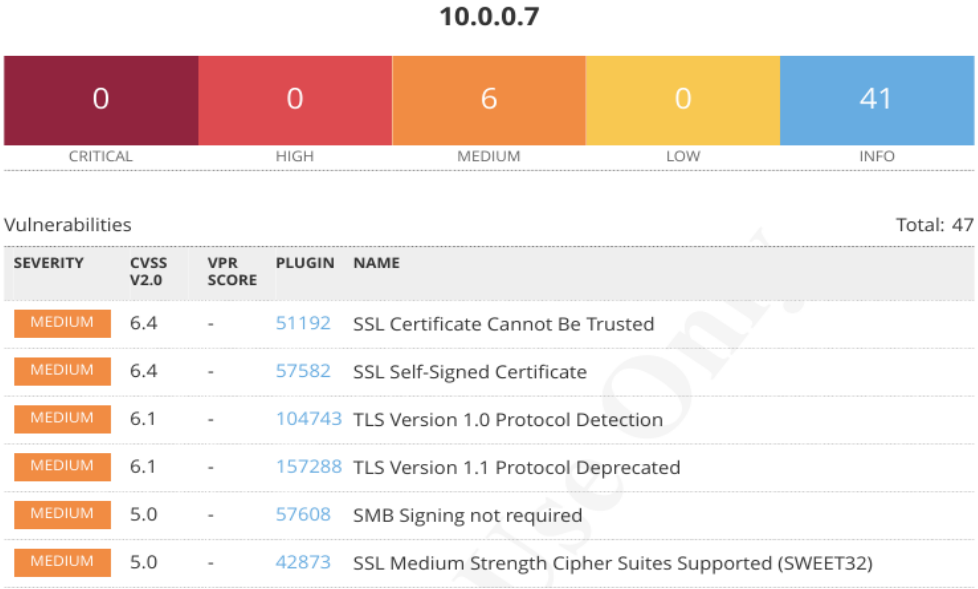
The 994 ports scanned but not shown below are in state: **filtered**

- 994 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])
22	tcp	open
	vulscan	VulDB - https://vuldb.com: No findings MITRE CVE - https://cve.mitre.org: [CVE-2010-5107] The default configuration of OpenSSH through 6 [CVE-2010-4478] OpenSSH 5.6 and earlier, when J-PAKE is enable [CVE-2009-2904] A certain Red Hat modification to the ChrootDi [CVE-2008-4109] A certain Debian patch for OpenSSH before 4.3p [CVE-2008-3844] Certain Red Hat Enterprise Linux (RHEL) 4 and [CVE-2008-3259] OpenSSH before 5.1 sets the SO_REUSEADDR socke [CVE-2008-1657] OpenSSH 4.4 up to versions before 4.9 allows r [CVE-2008-1483] OpenSSH 4.3p2, and probably other versions, al

Figura 19. Vulnerabilidades detectas del servicio OpenSSH sobre Windows Fuente: elaboración propia

La prevención en la aparición de este tipo de vulnerabilidad consiste en tener actualizada la versión del servicio SSH a la más reciente, a su vez habilitando únicamente los cifrados y algoritmos de comunicación mas robustos, deshabilitando los que son mas débiles evitando alguna brecha que pueda aprovechar la debilidad en este servicio para materializar algún ataque.



10.0.0.7

0	0	6	0	41
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 47

SEVERITY	CVSS V2.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.4	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	-	57582	SSL Self-Signed Certificate
MEDIUM	6.1	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.0	-	57608	SMB Signing not required
MEDIUM	5.0	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

Figura 20. Vulnerabilidades asociadas al servicio OpenSSH identificadas en Nessus
Fuente: elaboración propia

Los reportes completos de los análisis realizados, tanto externo como interno, se adjuntan como anexos a este documento

Recomendaciones

- En lo posible, seguir los lineamientos de seguridad de Azure, estos pueden ayudar a minimizar la aparición de vulnerabilidades en los servicios desplegados.
- Para cada vulnerabilidad identificada, y según su código CVE, tomar las medias necesarias para realzar mitigación de las mismas, se puede realizar siguiendo las recomendaciones documentadas por CVE o las expresas en el reporte de vulnerabilidades que genera la aplicación como Nessus.
- Incrementar seguridad de la plataforma implementado, además de los servicios de operación, reglas estrictas de firewall en la separación de las subredes, acceso a través de VPN, y motor de antivirus, ya sea externo o incorporado con la solución de Azure.
- Para la infraestructura desplegada es importante contar con respaldos que garanticen la continuidad de la operación, ya sea implementando o contratando proceso de replicación con el mismo proveedor de nube Azure, teniendo una contingencia de la

infraestructura y los datos en otra nube alterna como AWS, o en su defecto sobre infraestructura propia On-premises, esto previamente evaluados los costos, beneficios y criticidad de los servicios expuestos.

5. CONCLUSIONES

A pesar de que en la actualidad existen varias plataformas de la nube como lo son AWS, AZURE, ALIBABA o GOOGLE CLOUD, se eligió Azure para trabajar en este proyecto por la facilidad del soporte que se cuenta dentro de la misma herramienta, además, debido a la popularidad que está teniendo esta plataforma es sencillo obtener consultoría o asesoría relacionada con expertos cercanos, adicionalmente Azure tiene documentación y cursos en español y de manera gratuita, por ejemplo, al implementar un recurso, este nos da la opción de revisar la documentación o cursos relacionados al proceso que se está ejecutando.

Aunque Microsoft Azure cuenta con su propia herramienta para el análisis de seguridad y vulnerabilidades (Microsoft Defender for Cloud), el análisis que realiza esta herramienta se enfoca en características propias de Azure y recomendaciones basadas en soluciones adicionales de esta nube, implicando mayores costos de operación para la infraestructura. El análisis externo con herramientas de hacking ético independientes permite la autonomía y objetividad sobre el proceso de pentesting con identificación clara de vulnerabilidades recomendaciones y remediación.

Independiente al proceso de análisis de vulnerabilidades, la implementación de la infraestructura en una nube como la de Microsoft Azure, puede llegar a acarrear costos no planificados para la organización si no se realiza exhaustivamente la planificación de lo que se desea desplegar y evaluación de precios de los servicios ofrecidos por la plataforma. En este sentido se debe evaluar muy bien los pros y contras, no solo a nivel de seguridad de la información, también a nivel de procesamiento y recursos necesarios a utilizar como servicio en la nube para una migración de la infraestructura tecnológica en cualquier organización, en general, es posible que mantener una infraestructura tecnológica en la nube, por costos, no sea viable para las pequeñas empresas.

La instalación en Azure aunque en ciertos componentes son fáciles de desplegar esta tiene términos propios y algunos dispositivos que necesitan cierto conocimiento específico en la plataforma para su configuración y despliegue lo cual se deben realizar con profesionales capacitados, certificados o que tengan conocimiento en este tipo de implementación acarreando un costo adicional asociado a recurso humano.

Con respecto a las herramientas usadas para el escaneo de vulnerabilidades, identificamos que NMAP es bastante robusta y completa, pero requiere un gran esfuerzo en cuanto a la documentación disponible y el gran número de opciones y parametrizaciones que esta permite hacer, desde simple exploración, hasta un escaneo bastante agresivo sobre la red,

ahondado en que la herramienta se ejecuta a nivel de línea de comando lo cual hace más difícil su utilización para quien no está familiarizado con el uso de terminal de Linux, en contraste, la herramienta Nessus tiene facilidades de instalación, un ambiente gráfico amigable y los reportes generado son de fácil interpretación, su única desventaja con repto a NMAP es que Nessus es una aplicación de pago, para la ejecución de Nessus en este proyecto se usó el trial de 7 días.

Los resultados del análisis de vulnerabilidades muestra que la infraestructura en la nube puede llegar a ser igual de vulnerable o más que una implementación One-premises, ya que los servicios en la nube están altamente expuestos, si no se realizan las configuraciones pertinentes se pueden materializar ataques a los servicios, por consiguiente, la seguridad perimetral es uno de los factores más importantes a tener en cuenta, se debe segregar la red en zonas privadas y públicas, reforzando sus respectivas reglas de firewall, antivirus y VPN para acceso a recursos de la red privada, además se debe mantener las actualizaciones, parches de seguridad de sistemas operativos, así como seguir las recomendaciones de seguridad del proveedor del servicio en la nube y realizar hardening de los elementos que componen el ambiente..

En el escaneo externo de vulnerabilidades se identificaron múltiples sistemas y servicios expuestos asociado a dirección pública de la VPN, lo cual evidencia que a través de la URL de esta VPN, no solo se está exponiendo la infraestructura contratada, también se está exponiendo otras infraestructuras contratadas con la nube de Azure, a su vez, en los resultados de las pruebas internas se obtuvo información en el servidor de directorio activo, el sistema operativo está configurado la IP y MAC del equipo, igual para el caso de la base de datos muestra la versión de la misma y el sistema operativo donde está instalada y así para cada uno de los servicios que se implementaron en esta infraestructura.

A pesar de que las herramientas usadas de detección de vulnerabilidades son bastante invasivas a nivel de red y de sistemas operativos, la ejecución de estas no presento algún alertamiento de seguridad o bloqueo del proceso de escaneo por parte de Azure, adicional esto, en la validación de los términos y condiciones para la adquisición del servicio IaaS no existe algún limitante para poder realizar este tipo de análisis sobre esta nube por parte de quien contrata el servicio.

Como respuesta a la pregunta planteada al inicio de este artículo, una infraestructura de red implementada en la nube Azure como modelo IaaS, puede cumplir con todos los estándares de seguridad, siempre y cuando, se tengan medidas adoptadas en cuanto a seguridad perimetral, las cuales pueden ser contratadas con la misma plataforma o incorporadas de manera foránea, también incorporando buenas prácticas en cuanto actualizaciones seguridad de máquinas, implementación de antivirus y análisis de seguridad periódicos como el realizado en este proyecto.

El modelo de infraestructura usado en este proyecto puede ser ampliado en un futuro para probar otros servicios como APIs, ejecución de contenedores o servicios de gestión de usuarios, esto, realizando actualizaciones y ampliando servicios en lo ya implementado. En otra dirección sería posible también hacer un énfasis más profundo en la totalidad de los resultados de los reportes de vulnerabilidades arrojadas por las dos herramientas NMAP y Nessus, presentando estrategias y planes de mitigación completos para el aseguramiento de toda la infraestructura desplegada. Este proyecto también puede servido de comparación para un estudio similar usando otras plataformas en la nube como Google Cloud, AWS o Oracle Cloud.

FINANCIAMIENTO

Los únicos costos asociados a la ejecución de este proyecto corresponden a suscripción contratada con Azure, necesaria para poder implementar la infraestructura con los componentes adecuados para hacer válidas las pruebas de intrusión y así obtener los datos más verídicos posibles en el análisis de vulnerabilidades, estos costos son financiados con recursos propios.

Posterior la ejecución de las pruebas y el escaneo de vulnerabilidades la infraestructura es desmontada de la plataforma de Azure para evitar costos adicionales.

REFERENCIAS

Acevedo, N. Q. (2022). Seguridad y privacidad en la Nube, fortalezas y vulnerabilidades: Recomendaciones para tener en cuenta con los proveedores de servicios de la nube. *Universidad de Los Andes*.

Beatriz P. de Gallo1, H. B.-G. (2022). Auditoría de vulnerabilidades de seguridad de una arquitectura de procesamiento analítico basada en Azure. *SEDICI Univercida nacional de la Plata*.

BONFANTE, L. E. (2019). RECOMENDACIONES DE SEGURIDAD PARA LOS SERVICIOS DE COMPUTACIÓN EN LA NUBE, A PARTIR DE LOS ESTÁNDARES Y MODELOS DE SEGURIDAD DE LA INFORMACIÓN .

Carlos Manual Fernandez, M. R. (2015). Privacidad elevada en la nube.

Carrasco, u. d. (2014). LOS PROBLEMAS ESTRUCTURALES EN EL PLANTEAMIENTO DE LA CIBERSEGURIDAD. *DIALNET*.

CUESTAS, J. A. (2019). META-ANALISIS DE VULNERABILIDADES Y GESTIÓN DEL RIESGO EN ARQUITECTURAS CLOUD. *UNIVERSIDAD CATÓLICA DE COLOMBIA*.

CVE. (2023). *CVE*. Recuperado el 08 de 06 de 2023, de https://cve.mitre.org/cgi-bin/cvename.cgi

Diego Jara, P. C. (2017). Propuesta metodológica de evaluación de seguridad para aplicaciones deMobile Cloud Computing.

Evelin Pilar Díaz Rodríguez, J. A. (2022). PROPUESTA ARQUITECTURA DE SEGURIDAD PARA ORGANIZACIONES QUE UTILICEN LOS PRINCIPALES MODELOS DE SERVICIOS DE INFORMÁTICA EN LA NUBE.

Fuentes, N. L. (2014). COMPUTACIÓN EN LA NUBE. *Mundo Fesc*, 46 -51.

Guevara Jimenez, D. M. (2022). Diseño de una plataforma cloud basado en IAAS para un empresa de seguros.

Mario Casasola Robles (cloudMIDDLEtrust), M. S. (2014). *La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo.* Toluca, Mexico: CIDE.

Microfost. (02 de 03 de 2023). *¿Cómo funciona Azure?* Obtenido de https://learn.microsoft.com: https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/get-started/what-is-azure

Muñoz-Calderón, P. F.-M. (2020). Computación en la nube, la infraestructura como servicio frente al modelo On-Premise.

O, R. H. (2011). CLOUD COMPUTING Y SEGURIDAD: DESPEJANDO NUBES PARA PROTEGER LOS DATOS PERSONALES. *DIALNET*.

Pavón, A. S. (2022). Metodología a seguir para realizar tests de intrusión sobre entornos AWS.

Pereda, A. G. (2019). Pruebas de penetración y análisis de vulnerabilidades.

Salazar, V. H. (2016). Seguridad y protección de la Información en la Nube de Cómputo.

startechup. (2 de marzo de 2023). *PRUEBAS DE PENETRACIÓN EN LA NUBE: ¿QUÉ NECESITA SABER?* Recuperado el 27 de mayo de 2023, de https://www.startechup.com/es/blog/cloud-penetration-testing/#:~:text=Las%20pruebas%20de%20penetración%20en%20la%20nube%2C%20también%20conocidas%20como,que%20puedan%20abusar%20los%20hackers

tenable. (2023). *NESSUS*. Recuperado el mayo de 2023, de https://es-la.tenable.com/products/nessus

Trevejo, L. A. (2022). *Plan de continuidad de negocio de un file server ante un ataque de malware en Cloud.* Universidad Europea.