UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
ANÁLISIS DE VULNERABILIDADES DE LA SEGURIDAD DE ESTRUCTURAS VIRTUALIZADAS MEDIANTE PENTEST
Línea de Investigación:
Sistemas de Información e Informática
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autora:
Miryam Andrea Flor Castro
Tutor:
Mg. Pablo Marcel Recalde Varela

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Mg PABLO MARCEL RECALDE VARELA con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: Análisis de vulnerabilidades de la seguridad de estructuras virtualizadas mediante pentest.

Elaborado por: MIRYAM ANDREA FLOR CASTRO, de C.I: 1714030804, estudiante de la Maestría: SEGURIDAD INFORMÁTICA, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2023

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, MIRYAM ANDREA FLOR CASTRO con C.I: 1714030804, autora del proyecto de titulación denominado: ANÁLISIS DE VULNERABILIDADES DE LA SEGURIDAD DE ESTRUCTURAS VIRTUALIZADAS MEDIANTE PENTEST. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2023

_____

Firma

ORCID: 0009-0004-0288-5508

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Las infraestructuras de TI son una preocupación constante para las empresas en esta era digital. Con el crecimiento de las infraestructuras virtualizadas, es crucial asegurarse de que estas sean resistentes a ataques cibernéticos, con el fin de precautelar su seguridad informática.

Contextualización del tema

Los centros de datos se han visto directamente afectados por los requisitos de accesibilidad, disponibilidad, seguridad y la capacidad de aprovechar los servicios de forma continua y remota.

La adopción de tecnologías consolidadas como la virtualización, ha impulsado la descentralización de los centros de datos, dando lugar a la creación de nuevos entornos donde la información está más accesible. En este modelo, la información se envía a un único punto virtual, pero en realidad los datos se distribuyen en varios centros, lo que permite contar con una infraestructura distribuida, escalable y flexible.

La evolución de los centros de datos mediante la implementación de nuevas técnicas de virtualización plantea interrogantes sobre la capacidad de los sistemas de seguridad actuales para mitigar las amenazas y eliminar posibles vulnerabilidades.

A pesar de que la seguridad es un aspecto primordial en el diseño de cualquier tecnología, los sistemas de seguridad tradicionales no son adecuados para abordar los desafíos que plantea el nuevo paradigma de los centros de datos. Además, se están explorando las nuevas soluciones integrales de seguridad disponibles en el mercado. Por otro lado, se adopta un enfoque práctico al desarrollar y aplicar una guía de seguridad para un componente esencial de la virtualización. (Kennedy et al., 2019)

En base a lo expuesto, realizar una prueba de penetración (pentest) es beneficioso para identificar las vulnerabilidades presentes en los sistemas, redes o aplicaciones objetivo. Al simular ataques similares a los que podrían llevar a cabo los atacantes reales, es posible descubrir fallos de seguridad y debilidades antes de que sean aprovechados por personas malintencionadas. De esta manera, el pentest permite tomar medidas proactivas para fortalecer la seguridad y prevenir posibles brechas de seguridad. (Santana, 2022)

La virtualización permite crear múltiples máquinas virtuales (VM) en un único servidor físico, lo que ofrece beneficios como la consolidación de servidores, la flexibilidad, la

escalabilidad y el aislamiento. En este caso, se está trabajando con VMware Workstation, que es un hipervisor líder utilizado para la virtualización de servidores (VMware, 2020).

Proporciona una plataforma robusta y segura para virtualizar los recursos del servidor y ejecutar múltiples sistemas operativos simultáneamente. VMware ofrece una serie de características de seguridad y configuraciones que se deben tener en cuenta durante el pentest. (Reyes, 2022)

Problema de investigación

Se busca evaluar la seguridad de las infraestructuras virtualizadas mediante pruebas de penetración o analizar las vulnerabilidades comunes y las mejores prácticas de seguridad en amenazas y ataques de la seguridad de la información.

Con la creciente adopción de tecnologías de virtualización, como Vmware, HyperV5 y Proxmox, es fundamental garantizar la protección de los datos y la infraestructura. Se revisará en detalle los conceptos de análisis de vulnerabilidad y pentest en estructuras virtualizadas, y cómo estos servicios pueden ayudar a las organizaciones a fortalecer su seguridad digital.

La seguridad de los datos y sistemas sigue siendo una preocupación crítica, con el análisis de la información se pueden diseñar políticas de seguridad más eficaces para un mejor manejo de las infraestructuras virtualizadas.

¿Con un análisis de vulnerabilidades en infraestructuras virtualizadas, se puede mejorar la seguridad informática?

Objetivo general

Analizar la seguridad de las infraestructuras virtualizadas mediante pruebas de penetración, enfocándose en la plataforma VMware Workstation.

Objetivos específicos

Contextualizar los fundamentos teóricos de virtualización y pruebas de penetración.

Identificar las posibles vulnerabilidades en la configuración del hipervisor VMware Workstation, incluyendo los ajustes de seguridad y políticas de acceso.

Realizar pruebas de penetración en las máquinas virtuales alojadas en la infraestructura virtualizada, para la detección de vulnerabilidades en la configuración, aplicaciones y servicios implementados en dichas máquinas.

Vinculación con la sociedad y beneficiarios directos:

El resguardo de los datos personales y sensibles de los usuarios que interactúan con los sistemas y aplicaciones alojadas en la infraestructura es la prioridad al evaluar las vulnerabilidades que ayuda a salvaguardar la privacidad y la confidencialidad de la información. Tiene un impacto directo en la sociedad el garantizar que los sistemas y aplicaciones sigan funcionando sin interrupciones si se produce un ataque en la seguridad informática.

Al realizar un pentest y mejorar la seguridad de las infraestructuras virtualizadas, se protege la reputación y la confianza de la empresa en el mercado, demostrando su interés en la seguridad informática y la protección de sus datos.

Se contribuye al campo de la ciberseguridad puesto que los resultados del análisis pueden compartirse con la comunidad de seguridad y utilizarse para fortalecer las prácticas y medidas de protección en otros entornos similares.

En el Programa de las Naciones Unidas para el Desarrollo (PNUD) se describen los Objetivos de Desarrollo Sostenible (ODS), son 17 objetivos establecidos por las Naciones Unidas los que incluyen la pobreza, la desigualdad, el cambio climático, la degradación ambiental y la promoción del bienestar en todo el mundo.

Según PNUD (2023), los ODS que se relacionan con el análisis de vulnerabilidades en infraestructuras virtualizadas mediante pentest son: ODS 4 con el objetivo de enseñar a proteger la información en línea ya que en la actualidad se usan plataformas virtualizadas para la educación en varios ámbitos y el ODS 9 para contribuir a la creación de infraestructuras tecnológicas más seguras y confiables.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En este capítulo se describe el enfoque de este proyecto sobre la evaluación de la seguridad de infraestructuras virtualizadas basadas en hipervisor VMware ESXi 7.0 a través de la realización de pruebas de penetración, identificando y analizando las vulnerabilidades presentes en la configuración del hipervisor, máquinas virtuales y los servicios desplegados en el entorno virtualizado.

1.1. Contextualización general del estado del arte

Se pretende contribuir al enriquecimiento del panorama de la seguridad informática en el ámbito de la virtualización, proporcionando a las organizaciones herramientas y conocimientos vitales para salvaguardar su entorno digital en constante evolución.

La prueba de penetración (pentest) en infraestructuras virtualizadas con el hipervisor VMware Workstation es un tema relevante en el campo de la seguridad informática. En la última década, el crecimiento exponencial de dispositivos conectados a la red ha impulsado la evolución de las infraestructuras que los soportan. Se puede evidenciar en la Figura 1 como las empresas han ido cambiando a la virtualización a un ritmo acelerado que permite mayor control en el almacenamiento. (Smith, 2020)

Figura 1.
Virtualización de Servidores

Nota: Las empresas virtualizan sus entornos debido a la seguridad que proporciona.

Es necesario evaluar la seguridad de los sistemas informáticos como un todo siendo parte de la cultura organizacional, las evaluaciones de penetración implican que profesionales de seguridad informática éticos realicen ataques meticulosamente planificados dirigidos a la

estructura de seguridad de una compañía, con el propósito de detectar debilidades de seguridad que necesiten ser corregidas. Estas evaluaciones de penetración son componentes integrales dentro de un enfoque completo de seguridad para las aplicaciones web (Contreras, 2023).

1.2. Proceso investigativo metodológico

Dentro del marco metodológico que se aplica en el presente proyecto de análisis de vulnerabilidades en infraestructuras virtualizadas con VMware Workstation mediante pentest se detalla:

La metodología de revisión bibliográfica puede ser empleada en cualquier campo de estudio con el propósito de establecer la originalidad del tema investigado garantizando su autenticidad y a la vez facilitando la comprensión del trabajo que se está desarrollando (Gomez, 2014).

Figura 2.
Metodología Bibliográfica.

Nota: Elaborado por Autora.

La metodología de pentesting abre posibles escenarios de ataques cibernéticos para detectar debilidades en la seguridad que podrían ser explotadas por actores malintencionados. Con base en los resultados obtenidos, se elaborarán recomendaciones concretas para fortalecer las medidas de protección y reducir los riesgos potenciales en estas infraestructuras críticas. Mediante esta investigación, se pretende contribuir a la mejora de la seguridad de la información en entornos de virtualización, así como brindar a las organizaciones una comprensión más profunda de las amenazas y los procedimientos para mitigarlas. (Nowak, 2022).

La metodología experimental en el contexto de la seguridad de la información se puede aplicar con el fin de medir la eficacia de la seguridad implementada en infraestructuras virtualizadas mediante pruebas de penetración. (Calvo, 2021)

1.3. Análisis de Resultados

Es fundamental para extraer información significativa y fundamentada de las pruebas de pentest, lo que a su vez genera recomendaciones concretas para mejorar la seguridad en las infraestructuras virtualizadas.

La organización de los resultados de acuerdo con las categorías de vulnerabilidades, niveles de criticidad y sistemas afectados, garantiza un análisis acertado de la investigación de cómo las vulnerabilidades identificadas están relacionadas con la configuración específica del hipervisor y de las máquinas virtuales.

El análisis de vulnerabilidad en estructuras virtualizadas se refiere al proceso de identificación y evaluación de las debilidades y posibles riesgos de seguridad presentes en un entorno virtualizado. Esto implica examinar tanto los sistemas de virtualización en sí, como las máquinas virtuales y las aplicaciones que se ejecutan en ellas.

Se identifican los puntos débiles en la infraestructura virtualizada, como configuraciones incorrectas, software desactualizado o mal configurado, y posibles fallas de seguridad en las máquinas virtuales. Mediante el uso de herramientas especializadas, se realizan escaneos exhaustivos para detectar vulnerabilidades conocidas y potenciales, así como para analizar el grado de riesgo asociado a ellas.

Una vez finalizado el análisis, se genera un informe detallado que incluye las vulnerabilidades identificadas, su clasificación de riesgo y recomendaciones específicas para mitigar los riesgos y fortalecer la seguridad en la estructura virtualizada.

Tabla 1.
Comparativo de Virtualizadores

VIRTUALIZADOR	CARACTERÍSTICAS	DESCRIPCIÓN
VMware Workstation 17 Pro	Licenciamiento	Gratuito con características limitadas y versiones pagas con funcionalidades más avanzadas.
	Rendimiento y Escalabilidad	Sólido y su capacidad de escalar para entornos empresariales de gran envergadura.
	Ecosistema	Implementación en el sector industrial con una diversidad de soluciones y productos complementarios.

VIRTUALIZADOR	CARACTERÍSTICAS	DESCRIPCIÓN
	Gestión Centralizada	Herramientas de gestión como vCenter Server para administrar múltiples instancias de ESXi
	Seguridad	Seguridad avanzada y opciones de cifrado.
Microsoft Hyper-V	Integración con Windows	Hipervisor nativo de Windows y se integra estrechamente con el ecosistema de Microsoft
	Licenciamiento	Incluye con las ediciones Windows Server y tiene una variedad de funciones según la edición.
	Gestión y Administración	Herramientas como Hyper-V Manager y System Center Virtual Machine Manager (SCVMM) para la administración.
	Adopción Empresarial	Entornos donde Windows es la plataforma predominante.
	Ecosistema	Solido
Proxmox	Licenciamiento	Licencia de código abierto y tiene versiones de suscripción que agregan características adicionales y soporte.
	Interfaz Web	Interfaz web intuitiva para administrar tanto máquinas virtuales como contenedores.
	Virtualización y Contenedores	Virtualización de máquinas completas como contenedores LXC
	Escalabilidad	Entornos de tamaño mediano, requiere personalización para escenarios empresariales de gran envergadura
	Compatibilidad de Hardware	Limitada
KVM (Kernel-based Virtual Machine)	Licenciamiento	Código abierto
	Seguridad	Proporciona un entorno seguro para la virtualización
	Escalabilidad	Desde entornos de desarrollo hasta entornos empresariales de gran envergadura.
	Gestión de Recursos	Proporciona control granular sobre la asignación de recursos, como CPU, memoria y almacenamiento, a las máquinas virtuales.

Nota: Realizado por Autora

CAPÍTULO II: PROPUESTA

El pentest o prueba de penetración se basa en un enfoque ético y controlado de evaluación, implica simular ataques cibernéticos contra sistemas, redes, aplicaciones o infraestructuras las mismas que también pueden ser virtualizadas, con el fin de identificar y explorar vulnerabilidades de seguridad antes de ser víctimas de un ciberataque.

2.1 Fundamentos teóricos aplicados

¿Qué es el Pentest en Estructuras Virtualizadas?

El Pentest es un proceso de evaluación de seguridad que simula un ataque real sobre una estructura virtualizada. A diferencia del análisis de vulnerabilidad, el Pentest va más allá de la identificación de debilidades y se enfoca en probar las defensas de la infraestructura virtualizada y encontrar posibles rutas de ataque que podrían ser utilizadas por un atacante real (Santos, 2022).

Durante un Pentest, se utilizan técnicas y herramientas avanzadas para intentar explotar las vulnerabilidades identificadas en el análisis de vulnerabilidad. Esto puede incluir ataques de fuerza bruta, inyección de código malicioso, intentos de robo de información y otras técnicas comunes utilizadas por los atacantes (Torres, 2023).

Según Ortiz (2020), el objetivo del Pentest es evaluar la efectividad de las medidas de seguridad implementadas y detectar posibles fallas o debilidades que podrían ser explotadas por atacantes externos. A través de este proceso, se obtiene una evaluación más realista de la seguridad de la estructura virtualizada y se pueden tomar acciones correctivas para fortalecer aún más la seguridad.

El pentest lo realizan profesionales en seguridad cibernética denominados hackers éticos, los cuales imitan los pasos de un atacante real, siempre con el consentimiento del propietario de la red o sistemas a ser vulnerados con el objetivo de fortalecer las medidas de seguridad y proteger los recursos digitales. Dentro de pentest existen 3 tipos:

Caja Negra. Black Box Pentesting. También conocida como prueba a ciegas el hacker no recibe ninguna información a quien está atacando.

Caja Blanca. White Box Pentesting El hacker conoce toda la información y datos de la empresa simula como que alguien de la empresa realiza el ataque.

Caja Gris. Grey Box Pentesting. El hacker cuenta con cierta información a quien está atacando.

Figura 3.
Tipos de Pentesting

Nota: Realizado por Autora.

Diferencias entre el Análisis de Vulnerabilidad y el Pentest en Estructuras Virtualizadas

Aunque el análisis de vulnerabilidad y el Pentest comparten el objetivo general de fortalecer la seguridad en estructuras virtualizadas, existen diferencias significativas entre ambos servicios. Algunas de las principales diferencias son:

Enfoque: El análisis de vulnerabilidad su enfoque se dirige hacia la detección y clasificación de las debilidades presentes en la infraestructura virtualizada, mientras que el Pentest va más allá y busca explotar esas vulnerabilidades para evaluar la efectividad de las defensas.

Automatización vs. Acciones manuales: El análisis de vulnerabilidad es en su mayoría automatizado, utilizando herramientas especializadas para realizar escaneos y detectar vulnerabilidades. Por otro lado, el Pentest combina acciones automatizadas y manuales, ya que implica la ejecución de técnicas avanzadas y exploración de posibles rutas de ataque.

Amplitud vs. Profundidad: El análisis de vulnerabilidad tiene un enfoque más amplio, buscando detectar el mayor número posible de vulnerabilidades, sin profundizar en cada una de ellas. Por otro lado, el Pentest se centra en un número menor de vulnerabilidades, pero profundiza en cada una de ellas, tratando de adquirir la mayor cantidad de datos posibles y evaluar su real impacto en la seguridad de la infraestructura virtualizada.

Realización: Mientras que el análisis de vulnerabilidad puede ser realizado tanto por el equipo interno de la organización como por analistas externos, el Pentest generalmente se lleva a cabo por un equipo externo de pentesters especializados en pruebas de seguridad.

Esto se debe a la necesidad de una perspectiva imparcial y experta para evaluar la seguridad de la estructura virtualizada (Hernández y De la Cruz, 2022).

Figura 4.
Pentest VS Análisis de Vulnerabilidades

Nota: Elaborado por Autora.

El proceso de pentest generalmente sigue una metodología bien estructurada y estándar que involucra varias fases, como:

Escaneo y Reconocimiento de puertos

Es la fase de inicio para definir como se va a realizar la recopilación de datos mediante el ataque simulado. Con que herramientas se va a realizar el ataque para la obtención de información se puede usar software de escaneo de puertos.

Análisis de vulnerabilidades

En base a los datos obtenidos en la fase anterior se busca los puntos más débiles, para atacar al sistema.

Explotación controlada

En esta fase se simulan los ataques al sistema, en base a las vulnerabilidades encontradas infiltrándose en el sistema.

Post Explotación

En esta fase se realizan los informes con la finalidad de indicar a la empresa las vulnerabilidades encontradas y se tomen medidas de cómo actuar ante posibles amenazas.

Figura 5.
Fases de Pentesting

Nota: Elaborado por Autora.

Los resultados del pentest proporcionan a las organizaciones una visión clara de sus deficiencias de seguridad y les permiten tomar medidas proactivas para mitigar los riesgos y fortalecer sus sistemas.

Es importante también tener clara la diferencia entre análisis de vulnerabilidades y pentest, la evaluación de vulnerabilidades puede ser realizada por el personal interno de la empresa o por un analista externo, el Pentest es encomendado a un equipo externo. Se recomienda la asesoría de un especialista en seguridad de la información para comprender cuándo y cómo aplicar estos dos enfoques en la organización, es imprescindible la inversión tanto en la evaluación de vulnerabilidades como en el Pentest para resguardar la empresa, ya que la evaluación es altamente efectiva para mantener la seguridad, mientras que el Pentest examina de manera profunda los riesgos presentados.

En este análisis se debe resaltar las amenazas a las que están expuestos los sistemas de virtualización y de la misma manera conocer sus vulnerabilidades.

Entorno Básico de Pentest

Entorno Web Vulnerable. Sistema o aplicación web con debilidades de seguridad que pueden ser explotadas por atacantes para comprometer la confidencialidad, integridad o disponibilidad de datos y servicios. En la Tabla 2 se visualiza las debilidades del entorno web.

Tabla 2.
Entorno Web Vulnerable.

DEBILIDAD	CONSECUENCIA	SOLUCIÓN
Falta de Parches y Actualizaciones	Si el software y las aplicaciones no están actualizados con los últimos parches de seguridad, podrían contener vulnerabilidades conocidas que los atacantes pueden aprovechar.	Actualizar software y aplicación de manera constante
Inyecciones SQL	Una falta de validación adecuada en las entradas de usuario podría permitir a los atacantes ejecutar comandos maliciosos en la base de datos.	Blindaje de base de datos
Cross-Site Scripting (XSS)	Si no se valida o escapa el contenido de entrada, los atacantes podrían insertar scripts maliciosos que se ejecuten en el navegador de los usuarios.	Mantener protegida la red
Cross-Site Request Forgery (CSRF)	Falta de protección contra ataques que intentan hacer que un usuario realice acciones no deseadas sin su conocimiento.	Actualizar corta fuegos
Autenticación Débil	Contraseñas débiles o un proceso de autenticación inseguro pueden permitir que los atacantes obtengan acceso a cuentas.	Tener una política de contraseñas y cuentas de acceso
Fugas de Información	Configuraciones incorrectas pueden permitir el acceso no autorizado a información sensible.	Manejar políticas de seguridad
Falta de Control de Acceso	Si no se implementan controles adecuados, los atacantes podrían acceder a funciones o datos a los que no deberían tener acceso.	Implantar las políticas de seguridad de la información

Nota: Elaborado por Autora

Entorno del Atacante. Herramientas, conocimientos y circunstancias que un atacante utiliza para llevar a cabo actividades cibernéticas ilegales o perjudiciales, aquí el atacante planifica y ejecuta sus acciones con el objetivo de comprometer la seguridad informática. En la Tabla 3 se visualiza el Entorno del Atacante

Tabla 3.

Entorno del Atacante

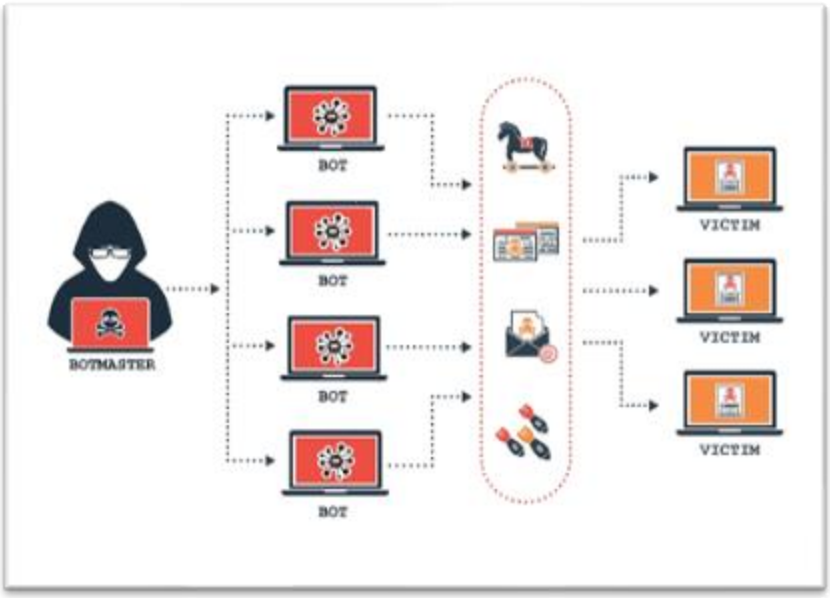
ELEMENTOS	CARACTERÍSTICAS	SOLUCIÓN
Herramientas y Software Malicioso	Los atacantes utilizan herramientas, como malware, exploits y kits de herramientas de hacking, para llevar a cabo sus actividades. Esto puede incluir virus, troyanos, ransomware y otras formas de software malicioso.	No abrir archivos sospechosos
Conocimientos Técnicos	Un atacante debe tener un conocimiento sólido de las tecnologías informáticas, redes, sistemas operativos y aplicaciones para identificar vulnerabilidades y explotarlas.	Mantener Redes blindadas
Recursos de Hardware	Pueden usar computadoras, dispositivos móviles y otros recursos de hardware para llevar a cabo sus ataques. Esto puede incluir sistemas comprometidos que forman parte de una red de bots para ataques distribuidos.	Educar a los usuarios
Infraestructura de Red	Los atacantes pueden utilizar redes privadas virtuales (VPNs) o sistemas de proxy para ocultar su ubicación y hacer que sea más difícil rastrear sus actividades.	Blindar la red
Circunstancias y Motivación	Tienen diferentes motivaciones, como obtener ganancias financieras, buscar reconocimiento en la comunidad hacker.	Mantener actualizados los sistemas
Conocimiento sobre Vulnerabilidades	Buscan nuevas vulnerabilidades en software, sistemas y redes para aprovecharlas en sus ataques.	Instalar corta fuegos
Técnicas de Ingeniería Social	Engañan a los usuarios para obtener acceso a información confidencial o sistemas.	Reportar incidentes

Nota: Elaborado por Autora

Tipos de Ataque

Denegación de Servicio (DoS). Este ataque busca agotar los recursos del sistema como el ancho de banda, capacidad de procesamiento o memoria lo que vuelve al sistema lento y no se puede acceder al recurso deseado. (Cloudfare, 2023).

Figura 6.
Diagrama de ataque DoS



Nota: Ataque de Distribuido de denegación de Servicio (Incibe, 2018).

Code Execution. Un atacante logra ejecutar su propio código malicioso en un sistema ejecuta comandos a distancia lo que puede darle el control a dicho sistema puede instalar un malware, un ransomware incluso robar la información. (Keepcoding, 2023).

Desbordamiento de pila (Stack Overflow). Se produce cuando un programa en ejecución agota la cantidad de espacio disponible en la pila que se usa para el almacenamiento de variables locales lo que puede provocar sobreescritura. (Spiegato, 2023).

Inyección SQL. Es una vulnerabilidad de seguridad en aplicaciones web que permite a los atacantes ejecutar comandos SQL no autorizados a través de entradas maliciosas en formularios u otras interfaces de entrada de datos en una aplicación, ocurre cuando los atacantes pueden manipular las consultas SQL enviadas a la base de datos (Mena, 2020).

Tabla 4.

Comparativo de Ataques informáticos

ATAQUES INFORMÁTICOS	TIPO	ACCIÓN
PHISHING	Ataque de suplantación de identidad mensajes de texto, mensajes en redes sociales o incluso llamadas telefónicas falsas	Robos de información como claves de acceso y contraseñas
TRASHING	Busca en la basura o en los desechos de una empresa información confidencial o datos sensibles que puedan ser utilizados para realizar ataques o comprometer la seguridad.	Obtención de información secreta o privada
MALWARE	Software diseñado para dañar, acceder de manera no autorizada o realizar acciones no deseadas en sistemas, redes o dispositivos.	Afecta a cuenta de usuario, seguridad de Internet, redes, dispositivos móviles.
DDOS	Se utilizan para inundar un sistema, red o servicio en línea con un gran volumen de tráfico, sobrecargándolo y dejándolo inaccesible para los usuarios legítimos.	Colapso en el servicio en línea impide el acceso y la publicación de información
ATAQUE MONITORIZACIÓN	Este ataque puede ser parte de una estrategia de ingeniería social, donde el atacante busca recopilar información a través de la observación de las acciones de los usuarios, los patrones de tráfico de red u otras señales disponibles.	Observación de la víctima y sus contraseñas personales

Nota: Realizado por Autora

Herramientas de pentesting.

Según Bortnik (2020) entre las herramientas de pentesting se tiene:

NMAP.

Es una aplicación de acceso gratuito y de código abierto que nos permite realizar un escaneo de los puertos, detección de equipos, servicios y sistemas operativos. Ofrece una variedad de técnicas de escaneo, desde el simple escaneo de ping para determinar qué dispositivos están activos en la red, hasta escaneos más avanzados como escaneos de puertos para identificar qué servicios están disponibles en cada dispositivo y escaneos de scripts para detectar vulnerabilidades conocidas en sistemas y aplicaciones.

METASPLOIT FRAMEWORK.

Permite la explotación de las vulnerabilidades, es una herramienta de código abierto utilizada para realizar pruebas de penetración y pruebas de seguridad en sistemas, aplicaciones y redes. Es desarrollado por Rapid7 y es una de las herramientas más utilizadas en el campo de la seguridad informática.

El Metasploit Framework se utiliza para identificar vulnerabilidades en sistemas y aplicaciones, y también puede ser utilizado para explotar estas vulnerabilidades con fines éticos y legales, como parte de pruebas de seguridad. Las principales características del Metasploit Framework incluyen:

Escaneo y Enumeración: Puede realizar escaneos de puertos y servicios en una red para identificar sistemas activos y sus servicios.

Exploits y Payloads: Exploits códigos que aprovechan vulnerabilidades y payloads cargas útiles que se ejecutan en sistemas comprometidos.

Post-Explotación: Permite la realización de actividades posteriores a la explotación, como el acceso remoto de sistemas comprometidos y la adquisición de datos adicionales.

Automatización: Puede automatizar tareas repetitivas y realizar acciones en secuencia, lo que ahorra tiempo durante las pruebas.

Personalización: Los usuarios pueden personalizar y crear sus propios exploits y payloads para adaptarse a situaciones específicas.

Gestión de Resultados: Proporciona opciones para generar informes y registrar las actividades realizadas durante las pruebas.

Tabla 5.

Comparativo de Herramientas de Pentest

HERRAMIENTA	DESCRIPCIÓN	CARACTERÍSTICAS
KALI LINUX	Diseñada para la seguridad informática, pruebas de penetración, auditorías de seguridad y hacking ético. Herramientas utilizadas por profesionales de la seguridad y hackers éticos para evaluar la seguridad de sistemas, redes y aplicaciones.	Herramientas de Seguridad Integradas, Personalización, Actualizaciones Constantes, Documentación Amplia, Uso Ético, Comunidad Activa
WIRESHARK	Es una herramienta de análisis de tráfico de red de código abierto que permite capturar y examinar el tráfico en tiempo real en redes y sistemas	Captura de Tráfico, Análisis de Protocolos, Filtrado y Búsqueda de paquetes, Análisis de Flujos de Datos, Estadísticas y Gráficos, Soporte para Múltiples Plataformas
SQLMAP	Es una aplicación de código abierto que detecta y explota vulnerabilidades de inyección de SQL en aplicaciones web y bases de datos. Dirigida para el uso profesional para identificar y detectar vulnerabilidades.	Detección de Inyecciones de SQL, Automatización de Ataques de SQL, Soporte para Diferentes Sistemas de Gestión de Bases de Datos, Explotación de Vulnerabilidades, Interfaz de Línea de Comandos y GUI
HYDRA	Herramienta de código abierto diseñada para realizar ataques de fuerza bruta y ataques de diccionario en sistemas y servicios que requieren autenticación. Es ampliamente utilizada por profesionales de seguridad y hackers éticos para probar la fortaleza de contraseñas y nombres de usuario en diversos protocolos y servicios	Ataques de Fuerza Bruta y Diccionario, Soporte para Múltiples Protocolos, Personalización de Ataques, Control de Velocidad, Informes de Resultados

Nota: Elaborado por Autora

2.2 Descripción de la propuesta

Pentest en Infraestructuras Virtualizadas

Los pentest en infraestructuras virtualizadas siguen una metodología específica para garantizar una evaluación exhaustiva de la seguridad. Mediante la presente propuesta se pretende garantizar que:

Los sistemas y aplicaciones estén actualizados con los últimos parches de seguridad y sean configurados adecuadamente para minimizar las posibles vulnerabilidades.

Se Implementen medidas de protección adicionales, como firewalls y sistemas de detección de intrusiones.

Realizar análisis de vulnerabilidad de forma periódica regular para identificar y solucionar cualquier debilidad antes de que sea explotada.

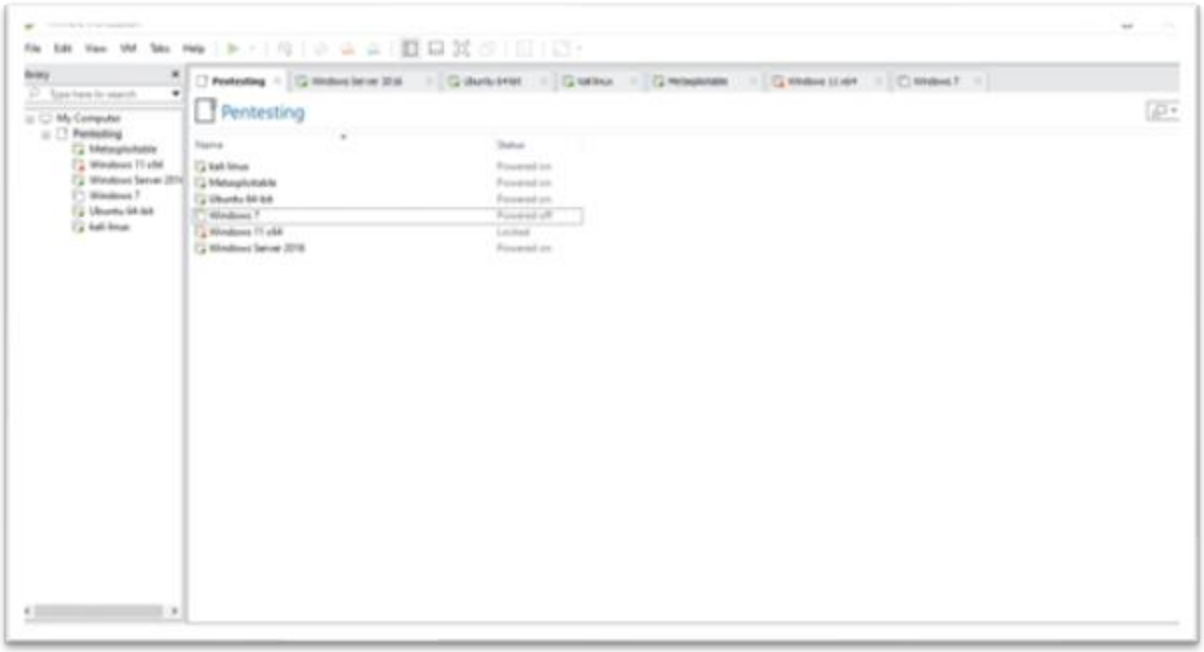
Capacitar al personal con buenas prácticas de seguridad y conciencia de las posibles vulnerabilidades.

A continuación, se detallan las etapas principales de esta metodología aplicadas al presente proyecto:

Recopilación de Información

La recopilación se realiza desde un escenario controlado en el que se instaló un virtualizador Vmware Workstation 17 Pro y se crearon 4 máquinas virtuales: Ubuntu 22.04, Windows Server 2016, Windows 11 y Kali Linux. Se va a analizar cuál de estos sistemas es menos vulnerable y más confiable con varias técnicas de hacking ético usando un entorno controlado garantiza que las pruebas sean en seguras. De esta manera se empezará con el Pentest se puede visualizar en la Figura 7 como se encuentra creado nuestro ambiente virtualizado y las máquinas virtuales creadas.

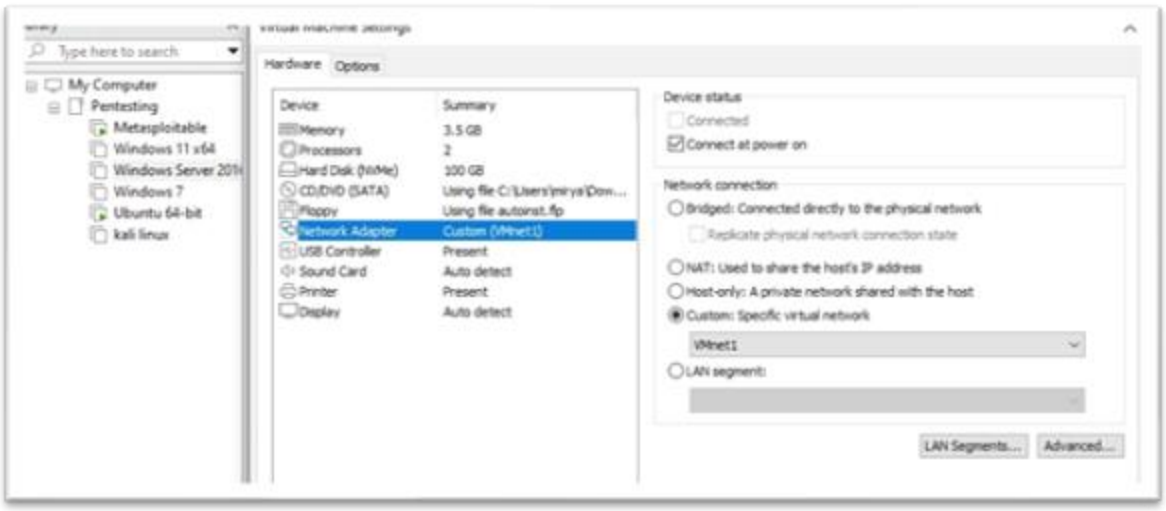
Figura 7.
Máquina Virtual VMware Workstation 17 Pro.



Nota: Elaborado por Autora.

Se crea una red VMnet1 mediante DHCP para todas las máquinas virtuales se realizan pruebas de ping con lo que se confirma que estén comunicadas y dentro de la misma red y a la vez se puedan comunicar de la misma manera Kali Linux que será la máquina atacante.

Figura 8.
Network VMnet1



Nota: Elaborado por Autora.

En la Tabla 6 se visualiza que las máquinas virtuales se encuentran dentro de la misma red VMnet1 y se detalla la ip asignada a cada una de las máquinas lo que nos permite saber exactamente la información de cada una de ellas al momento de usar la maquina atacante Klai Linux.

Tabla 6.
IP´S Asignadas a los Sistemas Operativos.

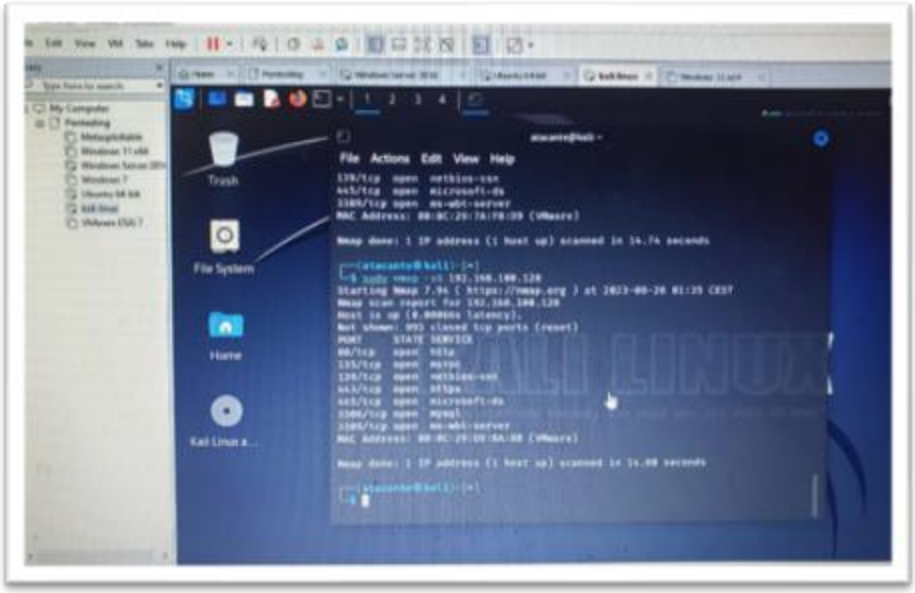
IP	SISTEMA OPERATIVO
192.168.100.128	WINDOWS SERVER 2016
192.168.100.131	WINDOWS 11 PRO
192.168.100.132	KALI LINUX
192.168.100.133	UBUNTU 22.04

Nota: Elaborado por Autora

Análisis de Vulnerabilidades

Se inicia con Kali Linux que es la máquina atacante, se utiliza Nmap para visualizar los puertos abiertos y que máquinas virtuales se encuentran en la red con una serie de comandos que permiten visualizar el sistema operativo y los servicios dentro de ellas.

Figura 9.
Nmap desde Kali linux



Nota: Elaborado por Autora.

Después del análisis con Nmap desde Kali Linux se lista en la Tabla 7 información relevante de cada máquina virtual como es el Sistema Operativo, los puertos abiertos, servicios asociados y Versiones. Lo que permite saber las vulnerabilidades de cada una para su explotación.

Tabla 7.

Puertos Abiertos

SISTEMAS OPERATIVOS	PUERTOS	SERVICIOS	VERSION
WINDOWS SERVER 2016	80/tcp	http	Microsoft IIS httpd 10.0
	135/tcp	msrpc	Microsoft Windows RCP
	139/tcp	netbios-sn	Microsoft Windows netbios-ssn
	443/tcp	ssl/http	Microsoft IIS http 10.0
	445/tcp	microsoft-ds	Microsoft Windows Server 2000 R2 microsoft ft-ds
	3306/tcp	mysql	MySQL 5.7.43-log
	3389/tcp	ms-wbt-server	Microsoft Terminal Services
	5985/tcp	http	Microsoft HTTPAPI http 2.0 (SSDP/UPnP)
	47001/tcp	http	Microsoft HTTPAPI http 2.0 (SSDP/UPnP)
	49664/tcp	msrpc	Microsoft Windows RPC
	49665/tcp	msrpc	Microsoft Windows RPC
	49666/tcp	msrpc	Microsoft Windows RPC
	49667/tcp	msrpc	Microsoft Windows RPC
	49668/tcp	msrpc	Microsoft Windows RPC
	49669/tcp	msrpc	Microsoft Windows RPC
	49670/tcp	msrpc	Microsoft Windows RPC
WINDOWS 11 PRO	135/tcp	msrpc	Microsoft Windows RPC
	139/tcp	netbios-ssn	Microsoft Windows netbios-ssn
	445/tcp	microsoft-ds	S/V
	3389/tcp	ms-wbt-server	S/V
UBUNTU 22.04	21/tcp	ftp	ProFTP 1.3.1
	22/tcp	Ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
	80/tcp	http	Apache http 2.2.8 ((Ubuntu) PHP/2.4.52 ubuntu5.10

Nota: Elaborado por Autora.

En la Figura 9 después del escaneo se presenta los sitios web de los sistemas operativos Ubuntu y Windows Server 2016 de los Servicios Web desde la máquina de Kali Linux se puede ver lo fácil que se accede a los mismos debido a sus puertos abiertos de esta forma podemos saber la información para acceder a nuestras maquinas objetivo.

Figura 10.

Servicios Web Expuestos

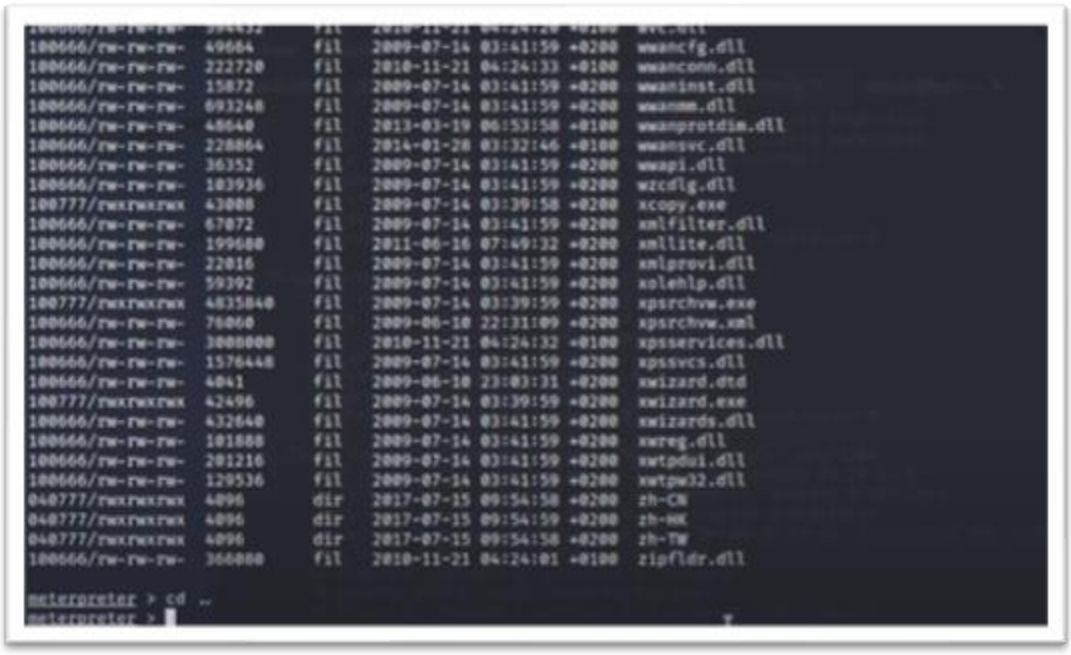
Nota: Elaborado por Autora

Explotación de Vulnerabilidades

Después de conocer las vulnerabilidades de nuestras máquinas se procede a la explotación de las mismas mediante Metasploit en Kali Linux. Se escoge uno de los puertos para acceder a las máquinas mediante eternalblue se realiza el exploit de la máquina de Windows a la que se accede al puerto 445 cambiando a la maquina atacante para poder ingresar a sus archivos, el acceso se pudo realizar y se puede ingresar a los directorios.

Figura 10.

Acceso a Windows 11 Pro

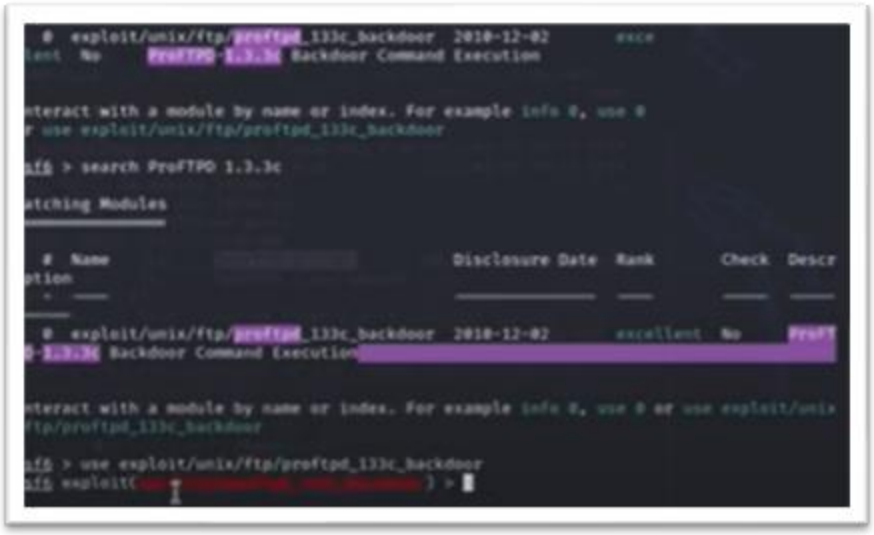


Nota: Control de Máquina Virtual Windows 11.

En Ubuntu se realiza el Exploit al puerto ftp se coloca la información de la máquina atacante ingresando a la máquina Ubuntu como administradores, por ssh podemos ver cuál es el usuario y contraseña en este caso usuario Ubuntu contraseña Ubuntu, mediante hydra.

Figura 12.

Exploit máquina Ubuntu



Nota: Servicio Ftp.

Dentro de las vulnerabilidades encontradas mediante la exploración se puede resumir que el servidor FTP permite leer y escribir archivos, se puede ejecutar código por los puertos expuestos y la información se encuentra vulnerable. Como se observa en la Tabla 8.

Tabla 8.

Vulnerabilidades Encontradas

SERVICIO	VULNERABILIDAD	DESCRIPCIÓN
ProFTPD	CVE-2015-3306	Permite leer y escribir archivos
SMBv1	CVE-2017-0143	Permite ejecutar código arbitrario
SSH	CVE-2019-11043	Información expuesta

Nota: Elaborado por Autora

Informe de Resultados

El presente informe detalla el pentesting realizado en 3 máquinas virtuales con distintos sistemas operativos con la herramienta Kali Linux como atacante y de lo analizado se puede observar que son vulnerables desde diferentes puertos y servicios lo que ha expuesto tanto la información de los sistemas operativos y usuarios como sus bases de datos instaladas, se recomienda mantener actualizados los servicios, configurar los puertos estrictamente necesarios de ser el caso de mantenerlos públicos, crear usuarios con accesos delimitados para evitar ingresos innecesarios tanto a bases de datos como a sistemas, utilizar un servidor de firewall para detectar y detener intrusiones maliciosas.

Se recomienda mantener actualizados los sistemas operativos con parches y las aplicaciones instaladas con últimas versiones.

La configuración de los sistemas debe realizarse de manera minuciosa al momento de su instalación. El análisis de vulnerabilidades debe realizarse de manera periódica y así solucionar cualquier debilidad antes de que se presente.

Capacitación constante al personal con buenas prácticas de seguridad y conciencia de las posibles vulnerabilidades.

El proceso de post explotación se realiza después de obtener acceso al sistema objetivo. En esta etapa, se analiza la información obtenida durante la fase de recolección de datos de los sistemas vulnerados. El propósito de la fase de post explotación es evaluar la importancia del dispositivo comprometido en un ataque y, principalmente, asegurar el control y el acceso continuo.

2.3 Valoración de la propuesta

El auge que ha tomado en la actualidad la virtualización es lo que ha motivado a realizar el presente proyecto con la finalidad de analizar las vulnerabilidades que puedan presentarse en entornos reales en las empresas por lo que el pentest es una metodología adecuada para garantizar la seguridad informática.

Después de completar la prueba de intrusión, es posible verificar que, mediante las herramientas y enfoques de la metodología propuesta, se logró evaluar, examinar y descubrir riesgos y debilidades que afectan la integridad de los datos.

La valoración de la propuesta cobra mayor significado debido a la ejecución de pruebas de intrusión mediante herramientas y técnicas metodológicas demostradas proporciona una vía sólida para evaluar la robustez del sistema de seguridad de una organización. Al identificar amenazas y vulnerabilidades que podrían exponer los datos a riesgos, esta propuesta se convierte en un recurso esencial para una evaluación exhaustiva de la postura de seguridad de las empresas.

La capacidad de analizar y comprender la naturaleza de las amenazas que podrían comprometer la seguridad de los datos es crucial para establecer una estrategia de mitigación eficaz. Mediante la aplicación de esta metodología, las empresas pueden obtener información valiosa sobre los puntos débiles de su sistema de información y, consecuentemente, mejorar su nivel de protección.

Además, la capacidad de situar el nivel de desempeño del sistema de información con respecto a la mitigación del riesgo y la toma de decisiones juega un papel importante para la gestión de la seguridad. Con la información proporcionada por estas pruebas, las organizaciones pueden adoptar medidas preventivas y correctivas pertinentes, lo que conlleva a una toma de decisiones informada y oportuna. La combinación de estas acciones no solo protege los datos de la empresa, sino que también garantiza la continuidad de sus operaciones en un entorno digital cada vez más complejo.

No es solo una herramienta para evaluar amenazas y vulnerabilidades, sino también como un catalizador para la toma de decisiones basada en la realidad de los riesgos de la seguridad informática. Con una base sólida y un enfoque metodológico riguroso, esta propuesta puede ser un recurso valioso para fortalecer la seguridad de la organización y resguardar sus activos digitales en un entorno de constante cambio y evolución tecnológica.

2.4 Matriz de articulación de la propuesta

En la presente matriz se puede visualizar los diferentes componentes del proyecto que han permitido alcanzar los objetivos planteados.

Tabla 9.

Matriz de articulación

Actividades		Recursos	Sustento teórico	Resultados
1	Creación de un entorno controlado de virtualización	Equipo de Hardware y software	Creación máquinas virtuales VMware	Evaluación de la Seguridad informática en entornos virtualizados.
2	Recopilación de Información y Análisis de vulnerabilidades	Máquinas Virtuales creadas en Vmware Workstation	Metodología de Pentesting.	Hallazgos y acciones de mitigación
3	Informe y Recomendaciones	Información Recopilada y Análisis de vulnerabilidades	Conocimientos técnicos en Seguridad Informática	Informe de Recomendaciones y Soluciones.

Nota: Elaborado por Autora.

CONCLUSIONES

El análisis de vulnerabilidades es un proceso continuo y en constante evolución. Las amenazas y las vulnerabilidades cambian con el tiempo, por lo que es importante revisar regularmente y actualizar las medidas de seguridad en las infraestructuras virtualizadas.

Este proyecto se ha desarrollado con el objetivo general de analizar la seguridad de infraestructuras virtualizadas a través de pruebas de penetración, centrándose específicamente en la plataforma VMware Workstation. Al alcanzar los objetivos establecidos y teniendo en cuenta la integración de los Objetivos de Desarrollo Sostenible (ODS), se ha logrado contribuir significativamente al ámbito de la ciberseguridad y la protección de datos en entornos virtualizados.

La contextualización de los fundamentos teóricos de la virtualización y las pruebas de penetración ha sentado las bases para comprender la importancia de abordar la seguridad en entornos altamente dinámicos y virtualizados.

Al identificar las posibles vulnerabilidades en la configuración del hipervisor VMware Workstation, se debe incluir ajustes de seguridad y políticas de acceso, se destaca la importancia de llevar a cabo una evaluación no solo de la funcionalidad, sino también la robustez de las soluciones de virtualización, la seguridad de VMware Workstation es un proceso continuo y debe ser parte de una estrategia de seguridad más amplia. Se debe evaluar y ajustar de forma regular la configuración para mantenerla al día con las mejores prácticas de seguridad y las últimas amenazas cibernéticas.

Al realizar pruebas de penetración en las máquinas virtuales alojadas en la infraestructura virtualizada, se ha conseguido detectar vulnerabilidades en la configuración, aplicaciones y servicios implementados en estas máquinas. Esto no solo demuestra la capacidad de las técnicas de pruebas de penetración para identificar debilidades, sino que también subraya la importancia de una postura de seguridad sólida y continua en todo el entorno virtualizado.

Es importante recalcar que la constante configuración y actualización que se realicen en los sistemas operativos es una práctica fundamental para mantener un alto nivel de seguridad informática. La evaluación de la seguridad en infraestructuras virtualizadas es una necesidad imperante debe ser de manera periódica.

RECOMENDACIONES

En base al análisis y conclusiones de este proyecto, se derivan las siguientes recomendaciones:

Mantenimiento Continuo de la Seguridad: La seguridad cibernética es un proceso constante y en evolución. Se recomienda que la empresa mantenga una vigilancia constante en la seguridad de sus infraestructuras virtualizadas, realizando pruebas de penetración de forma regular y manteniendo los sistemas actualizados con las últimas medidas de seguridad.

Implementación de Buenas Prácticas: Adoptar y aplicar buenas prácticas de seguridad desde el principio es esencial. Como el uso de contraseñas robustas, la segmentación de redes y la aplicación de parches de seguridad.

Formación y Concientización: Capacitar al personal en prácticas de seguridad informática es fundamental. La formación puede ayudar a prevenir errores humanos que podrían resultar en vulnerabilidades no deseadas.

Mantenimiento y actualización periódica: Actualizar los sistemas, aplicaciones y herramientas con los últimos parches de seguridad es esencial para prevenir debilidades ya identificadas que pueden ser aprovechadas por atacantes.

Gestión de Accesos: Crear un sistema de gestión de accesos y privilegios que limite el acceso a recursos y datos según los roles y responsabilidades de los usuarios. Esto reduce el riesgo de acceso no autorizado.

Evaluación de Terceros: Si la empresa utiliza proveedores de servicios o herramientas de terceros, asegurarse de que también cumplan con estándares de seguridad. Realizar pruebas de seguridad en sus sistemas antes de integrarlos en la infraestructura.

Gestión de Incidencias: Elaborar un protocolo de respuesta ante incidentes para saber cómo manejar situaciones de seguridad adversas de manera efectiva y minimizar los daños potenciales.

Auditorías Regulares: Realizar auditorías de seguridad regulares para evaluar y garantizar que las medidas de seguridad implementadas sigan siendo efectivas y estén actualizadas.

La monitorización de registros y la educación del personal en seguridad cibernética son prácticas importantes, junto con un plan de respuesta a incidentes y la colaboración con la comunidad de seguridad. La seguridad es un proceso continuo y proactivo en la configuración de VMware Workstation.

BIBLIOGRAFÍA

Bortnik, S. (2020). *revista.seguridad.unam.mx*. https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Calvo, A. (2021). *https://rutamaestra.santillana.com.co*. https://rutamaestra.santillana.com.co: https://rutamaestra.santillana.com.co/wp-content/uploads/2019/03/metodologias-experimentales.pdf

Cloudfare. (2023). *www.cloudflare.com*. www.cloudflare.com: https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/

Contreras, J. R. (05 de 2023). *https://rei.iteso.mx*. https://rei.iteso.mx/bitstream/handle/11117/9220/PAP1-2023P_L%C3%93PEZ-Contreras-JonathanR_Reporte-Final.pdf?sequence=1

Gomez, E. (2014). *www.scielo.org.co*. www.scielo.org.co: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0012-73532014000200021

Hernández, O. E., y De la Cruz, R. M. (2022). *https://repositorio.unprg.edu.pe*. https://repositorio.unprg.edu.pe: https://repositorio.unprg.edu.pe/handle/20.500.12893/11129

Incibe. (2018). *https://www.incibe.es*. https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos#

Keepcoding. (3 de julio de 2023). *keepcoding.io*. https://keepcoding.io/blog/que-es-la-ejecucion-remota-de-codigo/

Kennedy, D., O'Gorman, J., Devon, K., y Aharoni, M. (2019). *METASPLOIT.* HD Moore.

Mena, O. (2020). *http://repositorio.upea.bo*. http://repositorio.upea.bo/handle/123456789/210

Nowak, S. (28 de Noviembre de 2022). *nuclio.school*. nuclio.school: https://nuclio.school/que-es-el-pentesting/

Ortiz, A. M. (31 de 01 de 2020). *repository.unipiloto.edu.co*. epository.unipiloto.edu.co: http://repository.unipiloto.edu.co/handle/20.500.12277/6863

PNUD. (2023). *www.undp.org*. www.undp.org: https://www.undp.org/es/sustainable-development-goals

Reyes, S. (2022). *info.ingens-networks.com*. info.ingens-networks.com: https://info.ingens-networks.com/blog/2015/03/11/7-ventajas-de-virtualizar-servidores-con-vmware

Santana, J. J. (2022). *riull.ull.es*. riull.ull.es: https://riull.ull.es/xmlui/bitstream/handle/915/28744/Pentesting%20en%20entornos%20controlados.pdf?sequence=1&isAllowed=y

Santos, J. J. (28 de julio de 2022). *https://www.deltaprotect.com*. https://www.deltaprotect.com: https://www.deltaprotect.com/blog/que-es-pentesting

Smith, C. (Noviembre de 2020). *https://community.spiceworks.com*. https://community.spiceworks.com: https://community.spiceworks.com/blogs/marketing/3231-the-2020-state-of-virtualization-marketer-takeaways

Spiegato. (2023). *spiegato.com*. https://spiegato.com/es/que-es-un-desbordamiento-de-pila

Torres, G. I. (10 de 01 de 2023). *https://openaccess.uoc.edu*. https://openaccess.uoc.edu/handle/10609/147381

VMware. (2020). *docs.vmware.com.* docs.vmware.com: https://docs.vmware.com/es/VMware-vSphere/7.0/vsphere-esxi-701-installation-setup-guide.pdf

ANEXOS

ANEXO 1

Nombre de la Organización]
Dirección de la Organización]
Teléfono de la Organización]
Correo Electrónico de la Organización]
Fecha]

Nombre del Destinatario]
Título del Destinatario]
Dirección del Destinatario]
Teléfono del Destinatario]

Asunto: Permiso para Prueba de Penetración (Pentest)

Estimado/a [Nombre del Destinatario],

La organización [Nombre de la Empresa de Seguridad Cibernética], representada por [Tu Nombre], [Tu Título] solicita formalmente su permiso para llevar a cabo una prueba de penetración en los sistemas de nuestra organización.

Esta prueba de penetración se realizará con el objetivo de evaluar la seguridad de nuestra infraestructura y aplicaciones, identificar posibles vulnerabilidades y tomar medidas proactivas para mejorar nuestra postura de seguridad cibernética.

El Pentest se llevará a cabo en el siguiente período de tiempo: [Fechas programadas]. Durante este tiempo esperamos realizar pruebas exhaustivas en nuestros sistemas y redes.

Entendemos la importancia de mantener la disponibilidad y la integridad de nuestros sistemas y garantizamos que se tomarán las siguientes precauciones:

a. Se minimizarán las interrupciones al funcionamiento normal de nuestros sistemas.

b. Se evitarán daños permanentes a los sistemas.

c. Se respetarán las políticas y regulaciones de la organización.

d. Se proporcionará un informe detallado de los hallazgos y las recomendaciones después de la prueba de penetración.

Reconocemos que esta prueba de penetración puede exponer posibles debilidades y riesgos en nuestros sistemas, y estamos comprometidos a abordar y remediar cualquier hallazgo crítico de seguridad que se identifique durante el proceso.

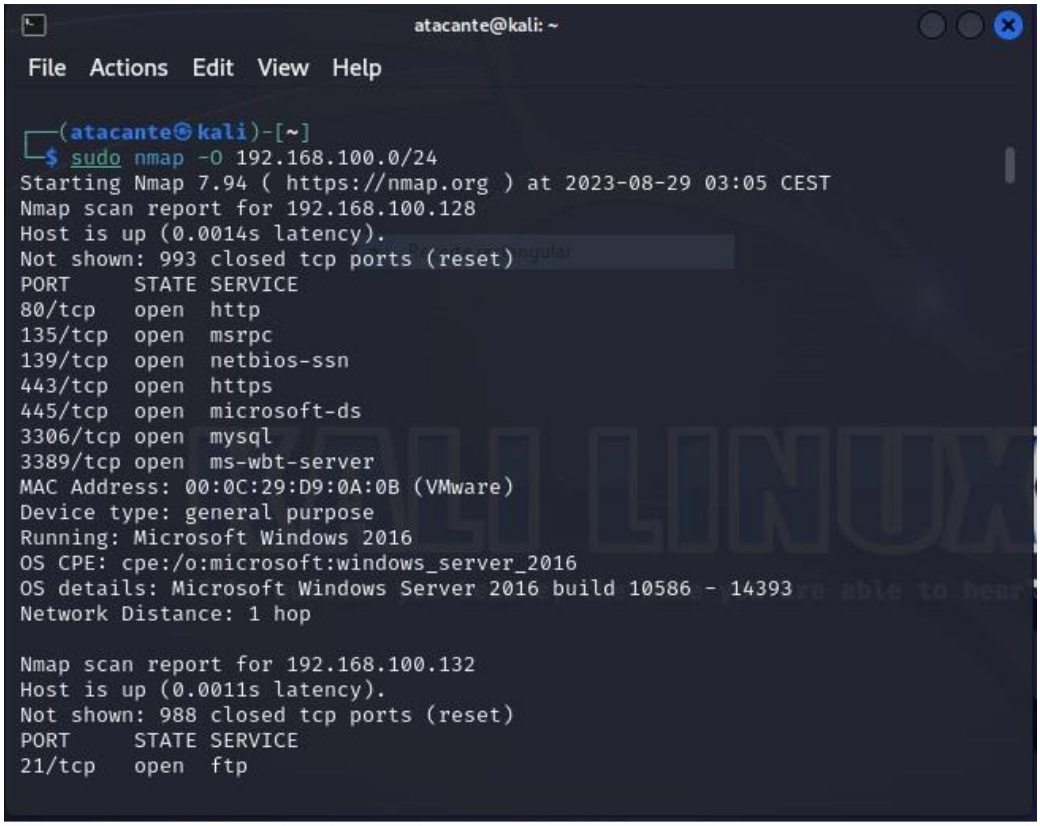
Agradecemos su cooperación y comprensión en este asunto y quedamos a su disposición para cualquier pregunta o inquietud que pueda surgir. Agradecemos su apoyo continuo a la seguridad de nuestra organización.

Por la presente, otorgamos permiso a [Nombre de la Empresa de Seguridad Cibernética] para llevar a cabo la prueba de penetración según lo descrito anteriormente.

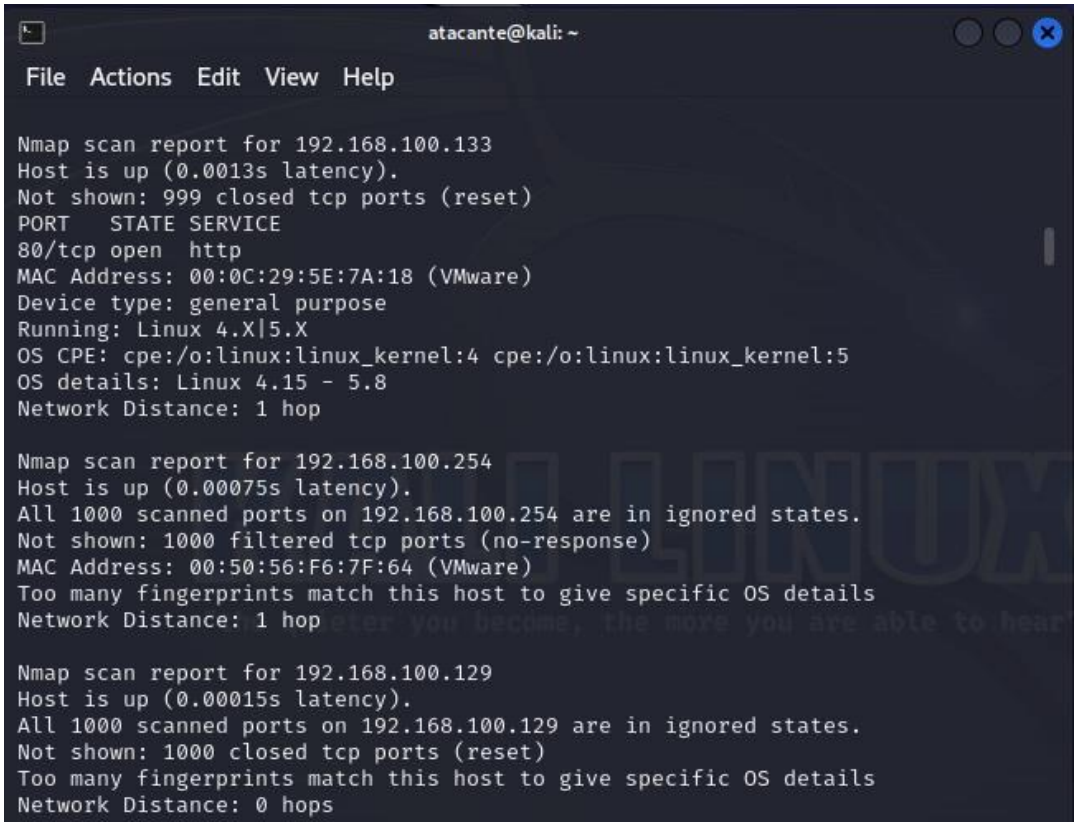
Atentamente,

Firma Digital de la Alta Dirección de la Organización]
Nombre del Firmante]

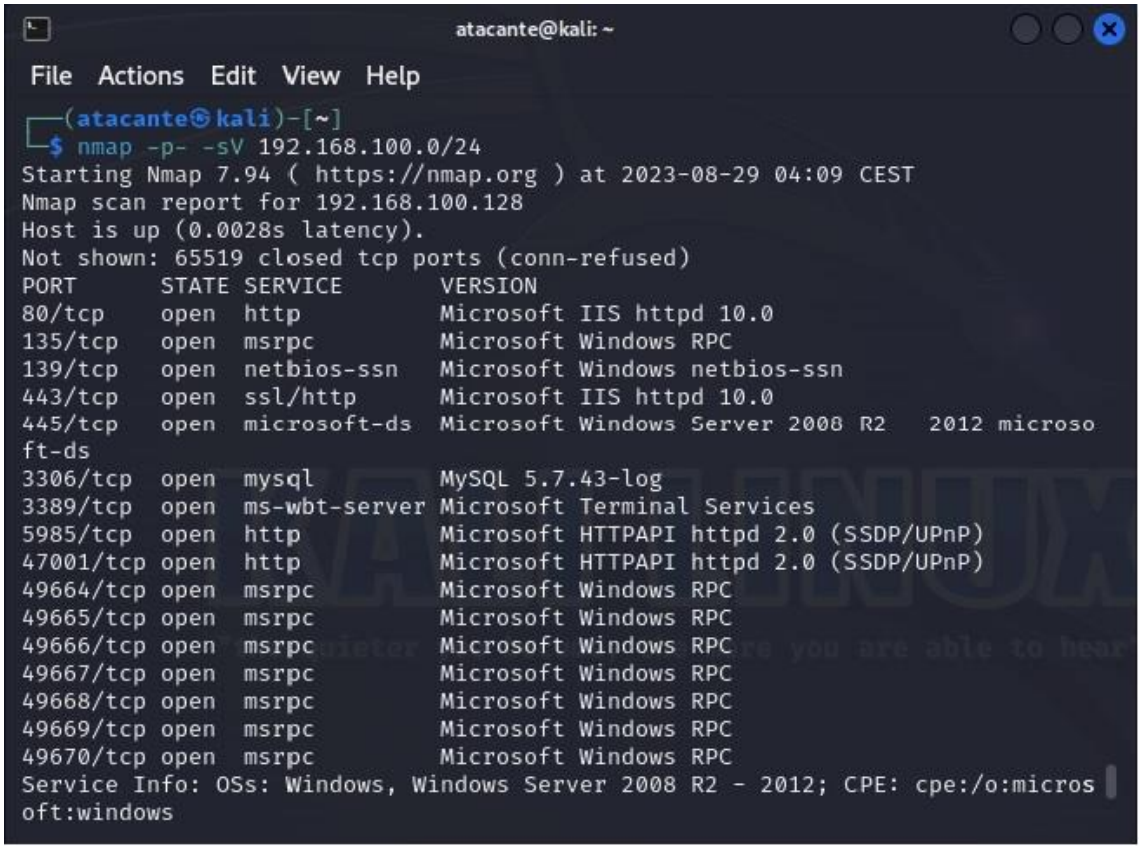
ANEXO 2



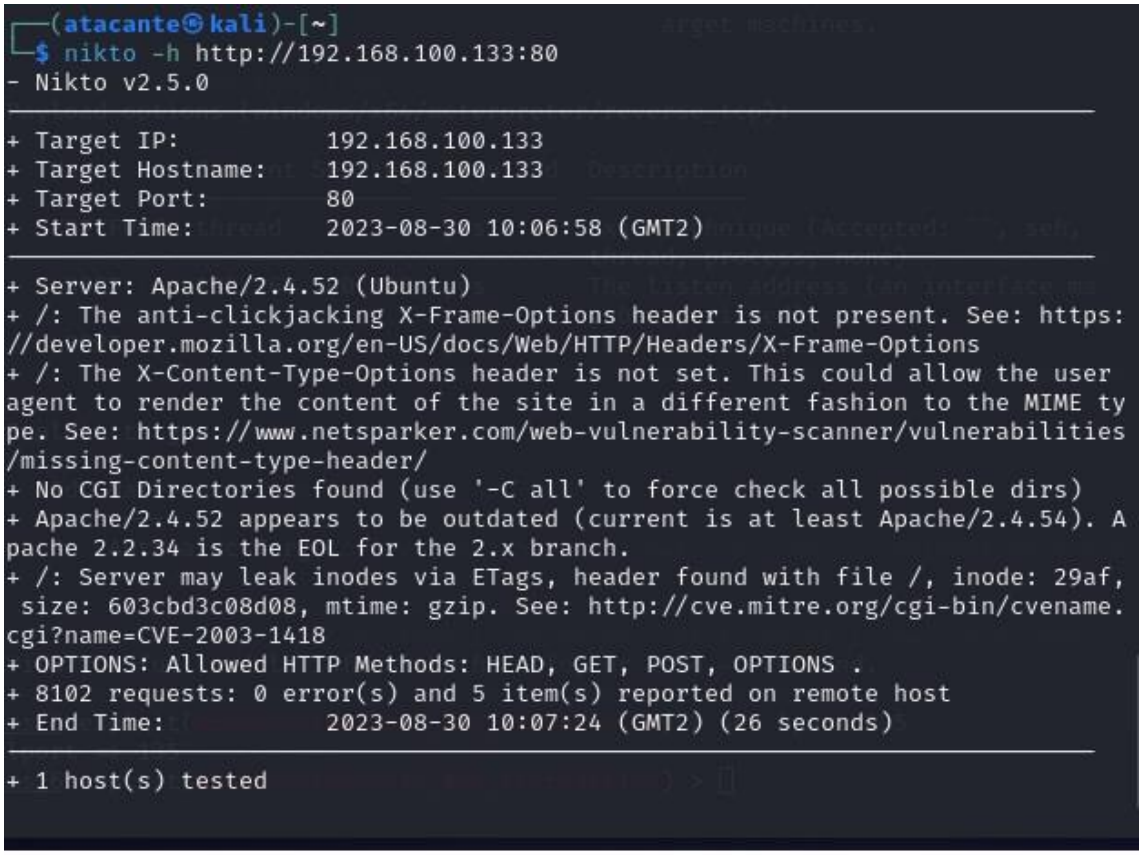
ANEXO 3



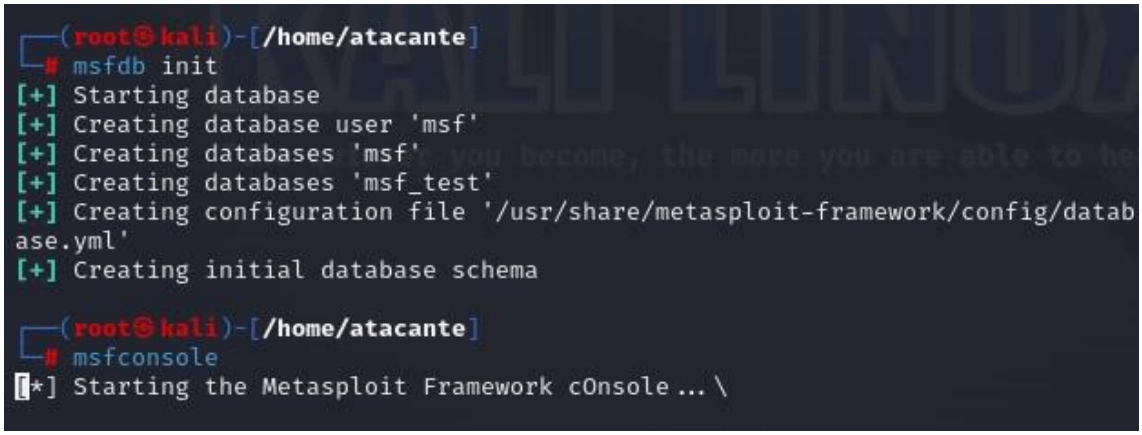
ANEXO 4



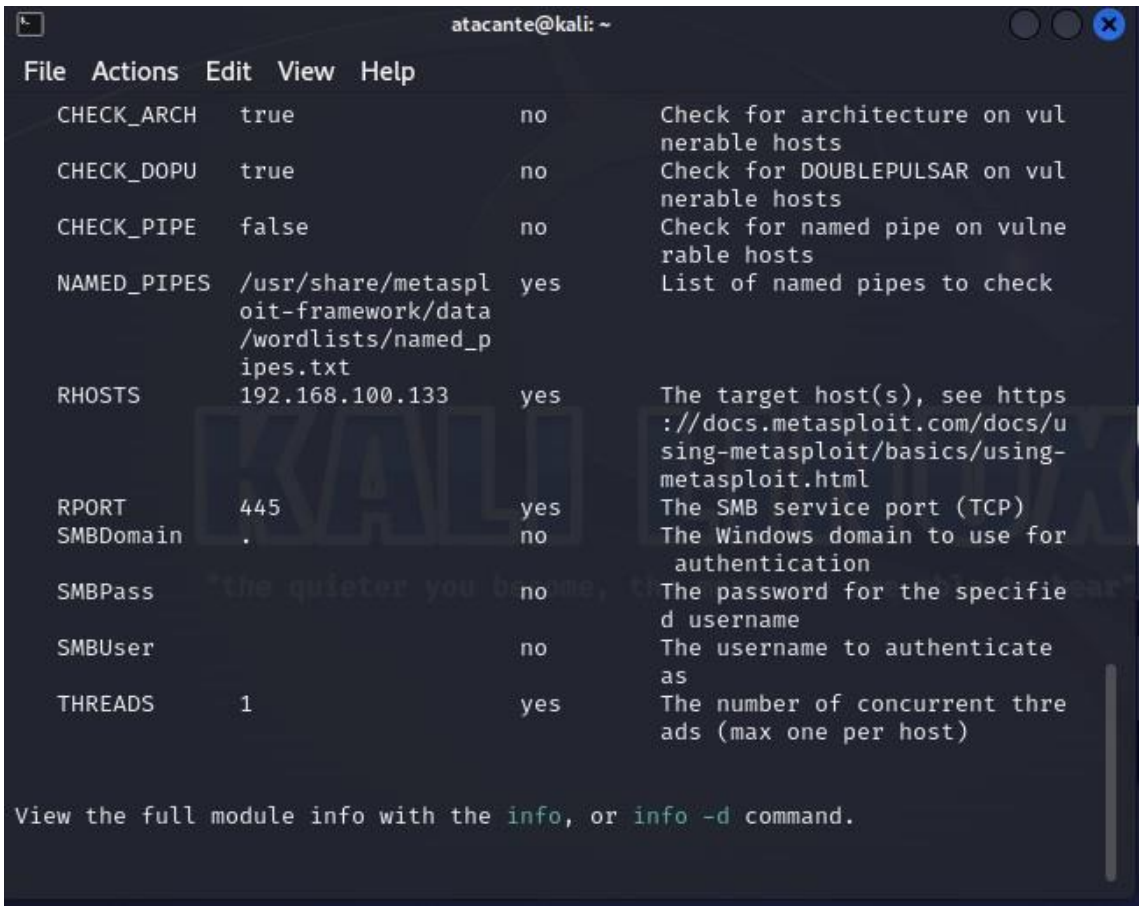
ANEXO 5



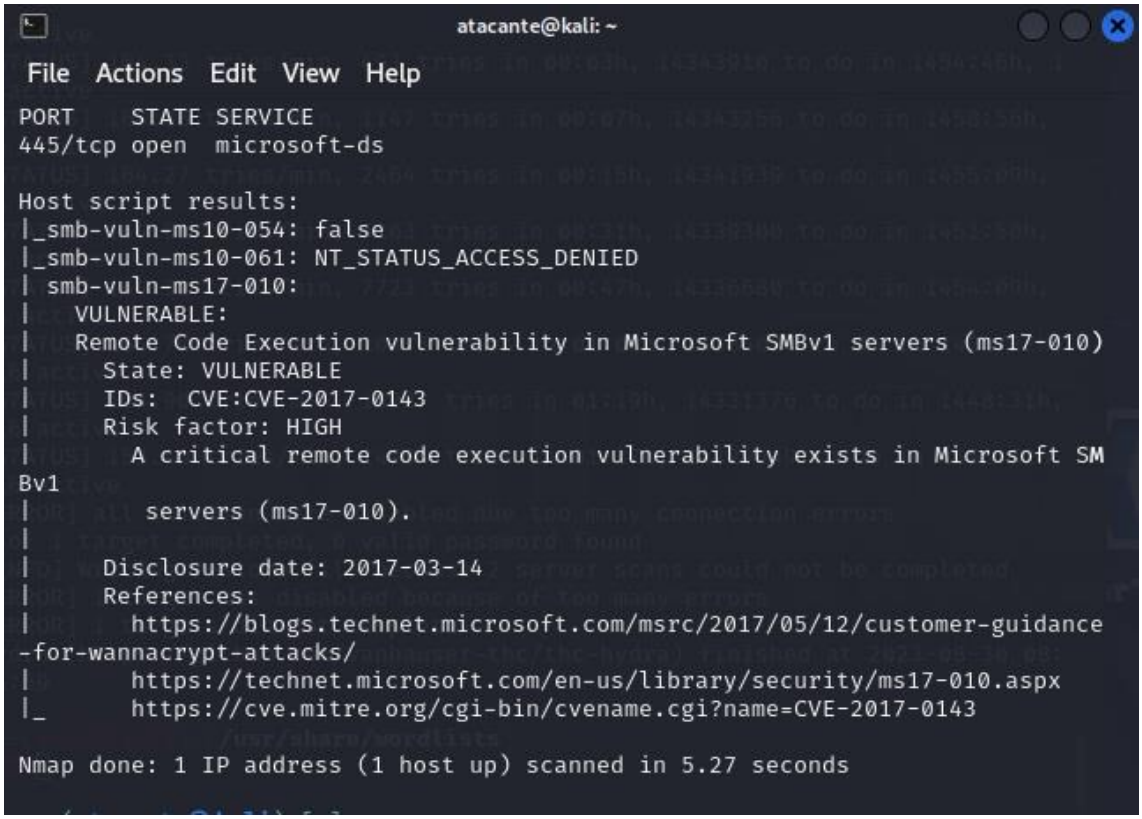
ANEXO 6



ANEXO 7



ANEXO 8


atacante@kali: ~
File Actions Edit View Help
PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SM
Bv1
| servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
| https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
-for-wannacrypt-attacks/
| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
Nmap done: 1 IP address (1 host up) scanned in 5.27 seconds

ANEXO 9

nforme de Prueba de Penetración

echa: septiembre de 2023

liente: XYZ Company

quipo de Pruebas de Penetración: [Nombre Experto]

esumen Ejecutivo:

a prueba de penetración se realizó en la infraestructura virtualizada de XYZ Company con el objetivo de valuar la seguridad de sus sistemas. Se identificaron varias vulnerabilidades críticas y se logró el acceso a istemas sensibles. A continuación, se resumen los hallazgos clave y se presentan recomendaciones para ejorar la seguridad.

allazgos Clave:
. Vulnerabilidad de Inyección de SQL: Se encontró una vulnerabilidad de inyección SQL en la aplicación web rincipal, lo que permitió el acceso no autorizado a la base de datos.
. Exposición de Servicios Innecesarios: Varios servicios no esenciales estaban expuestos en la red, lo que umentó la superficie de ataque y la posibilidad de explotación.
. Contraseñas Débiles: Se identificaron contraseñas débiles en varias cuentas de usuario, incluyendo la cuenta le administrador del sistema.
. Parches y Actualizaciones Pendientes: Algunos sistemas no tenían parches de seguridad actualizados, lo que ejó vulnerabilidades conocidas sin mitigar.
. Escalamiento de Privilegios Exitoso: Se logró el escalado de privilegios en un sistema de producción, lo que ermitió el acceso a datos sensibles.

cciones Tomadas:
. Se ha notificado al cliente sobre los hallazgos y recomendaciones.
. Se han proporcionado detalles técnicos sobre las vulnerabilidades y los pasos necesarios para remediarlas.
. Se han realizado pruebas adicionales para confirmar la mitigación de las vulnerabilidades identificadas.

ecomendaciones:
. Parches y Actualizaciones: Actualizar todos los sistemas y aplicaciones con los últimos parches de seguridad ara mitigar las vulnerabilidades conocidas.
. Seguridad en el Desarrollo: Implementar controles de seguridad durante el desarrollo de aplicaciones web ara prevenir futuras vulnerabilidades de inyección SQL.
. Eliminar Servicios Innecesarios: Deshabilitar o eliminar cualquier servicio no esencial para reducir la uperficie de ataque.
. Contraseñas Fuertes: Exigir políticas de contraseñas fuertes y cambiar las contraseñas débiles.
. Monitoreo Continuo: Implementar un sistema de monitoreo de seguridad para detectar actividades ospechosas y eventos de escalado de privilegios.

onclusiones:
a prueba de penetración ha identificado vulnerabilidades críticas en la infraestructura virtualizada de XYZ ompany. Es esencial que se tomen medidas inmediatas para remediar estas vulnerabilidades y mejorar la ostura de seguridad de la organización.

irma: Fecha de Entrega del Informe:

Experto en Pruebas de Penetración] septiembre de 2023

ANEXO 10

ANÁLISIS DE VULNERABILIDADES DE LA SEGURIDAD DE ESTRUCTURAS VIRTUALIZADAS MEDIANTE PENTEST

Evaluador: Alejandro Patricio Castrillón Sevilla

Ingeniero en Informática, Máster en estrategia y gestión de Ciberseguridad

Registro Senecyt: 3802207555

Jefe de Riesgo Tecnológico en Banco Internacional.

He revisado el tema "ANÁLISIS DE VULNERABILIDADES DE LA SEGURIDAD DE ESTRUCTURAS VIRTUALIZADAS MEDIANTE PENTEST" que menciona la Ing. Miryam Andrea Flor Castro, puedo mencionar que el tema planteado es interesante, dado que en la actualidad la mayoría de infraestructuras se enfocan la gestión virtualizada y de nube como una evolución del uso de infraestructuras físicas, es por ello que es de relevancia analizar la seguridad en las mismas con un enfoque holístico, con ello evitar posibles impactos en la confidencialidad, integridad y disponibilidad de las mismas de las empresas u organizaciones que las usen.

La interesada puede hacer uso de este documento para sus fines académicos pertinentes.

Alejandro Castrillón

Jefe de Riesgo Tecnológico - Proyectos

Atentamente

Ing. Alejandro Castrillón

CI. 171352468

Teléfono:0992939712

ANEXO 11

ANÁLISIS DE VULNERABILIDADES DE LA SEGURIDAD DE ESTRUCTURAS VIRTUALIZADAS MEDIANTE PENTEST

Evaluador: Erika Eliana Mora Flor

INGENIERA EN SISTEMAS DE COMPUTACION E INFORMATICA, *Registro SENECYT: 1040-2017-1829060*

LICENCIADA EN CIENCIAS DE LA EDUCACION MENCION INFORMATICA, *Registro SENECYT: 1006-2018-1997247*

MÁSTER EN GESTIÓN DE RIESGOS Y CIBERSEGURIDAD CON MENCIÓN EN CONTINUIDAD DEL NEGOCIO, *En proceso de registro del título (Maestría Internacional)*

JEFE DE CONTINUIDAD DEL NEGOCIO EN BANCO INTERNACIONA, *Cargo actual*

De mis consideraciones:

He revisado el tema *"ANÁLISIS DE VULNERABILIDADES DE LA SEGURIDAD DE ESTRUCTURAS VIRTUALIZADAS MEDIANTE PENTEST"* que menciona la ***Ing. Miryam Andrea Flor Castro***; por lo cual, puedo indicar que el tema planteado resulta útil, apropiado y está alineado a la realidad tecnológica mundial, cuya tendencia es el uso de infraestructuras virtualizadas. Por tal motivo, se hace indispensable el análisis de vulnerabilidades que permitan asegurar y proteger la información que es el principal activo de las empresas u organizaciones.

La interesada puede hacer uso de este documento para sus fines académicos pertinentes.

Atentamente,

Erika Eliana Mora Flor

Firmado digitalmente por Erika Eliana Mora Flor
Fecha: 2023.09.11 09:10:09 -05'00'

Ing. Erika Mora
CI. 1710328707
Cel. 0998004449