PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE INFORMACIÓN

"ANÁLISIS DE VULNERABILIDADES DE SERVIDORES VIRTUALIZADOS DE UNA RED EMPRESARIAL MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS DE SOFTWARE LIBRE".

AUTOR:

STALIN OMAR CABEZAS HERRERA

DIRECTOR:

MTR. JORGE ALARCÓN MENA

QUITO DM, 2022

DEDICATORIA

El presente trabajo se lo dedico con mucho amor a mi papá Danilo, a mi mamá Mayra, a mi hermanita Karolina quienes son mi apoyo incondicional, luz en mi camino y la mejor representación de amor familiar que necesito en mi vida.

Quiero dedicarlo también a una mujer muy importante en mi vida, Doménica Vallejo, quien ha sido una de las personas más maravillosas que puedo tener en mi vida, ella ha sido quien está para mí en los momentos difíciles que se han presentado, ayudándome a superar cualquier adversidad y estando para mi incondicionalmente; la vida no sería lo mismo sin ti.

Finalmente dedico este trabajo a mi Kiara quien fue un miembro más de mi familia, crecí con ella y era mi refugio, no fue solo una mascota, fue mi compañera de vida.

AGRADECIMIENTO

Quiero empezar agradeciendo a mis padres quienes han sido los pilares fundamentales tanto en mi formación personal como en mi formación académica; gracias a ellos puedo decir que estoy orgulloso de ser quien soy.

Agradezco a todos mis profesores de la Facultad por compartir su conocimiento conmigo. Con mención especial a Jorge Alarcón quien aparte de ser mi director del presente trabajo, es uno de los docentes quien supo exigirme académicamente para poder llegar a ser un excelente profesional con educación de calidad.

A mis amigos y compañeros de carrera agradezco los momentos compartidos dentro y fuera de las aulas de clase, fue un honor poder compartir risas con ellos.

RESUMEN

El presente trabajo presenta una propuesta acerca de cómo realizar un análisis de vulnerabilidades de software para servidores que se encuentren virtualizados dentro de una infraestructura de la red empresarial; para realizar el análisis se lo realizó mediante el uso de herramientas de Software Libre.

Dentro del capítulo 1 se describe la problemática, los objetivos del trabajo, el alcance y las limitaciones del presente trabajo. El capítulo 2 comprende el marco teórico en el cual se proporcionan conceptos sobre virtualización, seguridad de los sistemas informáticos, tipos de vulnerabilidades y herramientas para identificación de estas.

El capítulo 3 comprende el levantamiento y configuración de los servidores en un ambiente virtualizado para simulación de la red empresarial. Por consiguiente, el capítulo 4 presenta las herramientas de Software Libre que fueron utilizadas para el análisis de vulnerabilidades de software.

Ya identificadas las herramientas a utilizarse, en el capítulo 5 se prone el plan de ejecución para el análisis de vulnerabilidades de los servidores virtualizados anteriormente mencionados. La revisión de los resultados del análisis, son detallados en el capítulo 6 donde adicionalmente se justificará la metodología planteada del capítulo anterior.

Para finalizar, en el último capítulo se encuentran tanto las conclusiones a las que se llegaron con el desarrollo del trabajo como las recomendaciones que se pueden plantear respecto al tema seleccionado.

ÍNDICE

ÍNDICE DE FIGURAS, GRÁFICOS Y TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I: INTRODUCCIÓN

1. MARCO DE REFERENCIA.

1.1. JUSTIFICACIÓN.

Las redes empresariales que existen en la actualidad cuentan con infraestructura tanto de software como de hardware, en este aspecto, el software es el encargado de brindar los diferentes servicios al resto de equipos presentes en la red, sin embargo, este no está exento de presentar vulnerabilidades informáticas. Este trabajo de titulación permitió identificar y analizar de las diferentes vulnerabilidades de software que generalmente se presentan en los servicios que brindan los servidores de una red a todos sus equipos, mediante herramientas o software libre.

Es relevante y de vital importancia la identificación de vulnerabilidades de software en una red empresarial puesto que un reconocimiento temprano de estas ayudará a la toma de acciones correctivas, evitando así las posibilidades de fuga de información, acceso no autorizado de equipos que no pertenecen a la red o de cualquier otro posible ataque que se pueda realizar por alguna vulnerabilidad encontrada. Teniendo en consideración que las vulnerabilidades pueden presentarse de manera inesperada ya sea por algún error humano o actualizaciones del software, es indispensable contar con software que realice un análisis de estas de manera periódica.

Analizar las vulnerabilidades de software de los equipos que brindan servicios a la red empresarial es posible gracias a la utilización de distintas herramientas, como por ejemplo las de Software Libre; al ser de código abierto, hay la posibilidad de que este tipo de software tenga una mejora pronta en un menor tiempo, además, al ser software de libre acceso, es posible modificar su código fuente para que se adapten completamente a las necesidades de la empresa. Si bien es

conocido que este tipo de herramientas son para todo público, se opta por el uso de estas pues al ser de código abierto permite que la comunidad mejore o solucionen errores de versiones mediante los informes que estas proporcionan.

La factibilidad de llevar a cabo este proyecto es la detección temprana de vulnerabilidades de la red, la cual permitirá que los servicios que se entregan para los equipos de la red estén disponibles la mayor cantidad de tiempo posible, además, el proyecto beneficia a la detección temprana y rápida de fallas o vulnerabilidades gracias a las herramientas propuestas de Software Libre que se presentaron, ya que, se encontrarán en un monitoreo constante de los servicios proporcionados por la red, adicionalmente, estas herramientas permitieron un mayor control en la seguridad de la información de la empresa.

1.2. PLANTEAMIENTO DEL PROBLEMA.

Las pequeñas y medianas empresas (PYMES) que cuentan con una infraestructura de red, suelen tener una topología tradicional, las cuales se encuentra compuesta comúnmente de servidores quienes son los encargados de proporcionar los diferentes servicios a los usuarios pertenecientes a la red. Dentro de la red empresarial se maneja información la cual únicamente debe poder ser accedida por personal autorizado de la empresa, razón por la cual es indispensable que la seguridad que se encuentra implementada sobre la infraestructura informática debe garantizar que exista la menor cantidad de vulnerabilidades posibles.

Las vulnerabilidades que se presentan en los distintos sistemas informáticos de las empresas no se deben a un único factor específico, se presentan por varias circunstancias, las cuales pueden deberse (entre otras) a:

- Deficiente o inexistencia de seguridad en el diseño de los sistemas informáticos.
- Sistemas informáticos con compuertas traseras debido a su mala implementación.
- Incorrecta configuración para el uso de los sistemas informáticos.
- Uso de software malicioso que facilite un ataque.

Para empresas pequeñas y emergentes la posibilidad de realizar un análisis y mitigación de vulnerabilidades de software se ve comprometido posiblemente por el alto costo para la contratación de software especializado para realizar esta tarea, adicionalmente el costo se incrementa cuando los servicios requeridos para el análisis de vulnerabilidades es más profundo y requiere de más herramientas o del contrato de más servicios del paquete que se ha ofertado y no todas las empresas cuentan con el capital para realizar dicha inversión.

Una vez presentada y descrita la problemática hallada, se plantea como pregunta principal:

- ¿Cuál es el procedimiento por seguir para una correcta ejecución de un análisis de vulnerabilidades de los sistemas informáticos?

Y por consiguiente las preguntas secundarias:

- ¿Qué tipos de vulnerabilidades pueden encontrarse al realizar un análisis a los sistemas informáticos de una empresa?
- ¿Es viable la utilización de herramientas de Software Libre sobre herramientas de software de paga?
- ¿Qué garantiza que las herramientas de Software Libre a utilizarse son fiables?
- ¿Cómo interpretar los resultados de un análisis de vulnerabilidades a los sistemas informáticos?

- ¿Qué medidas se deben tomar para la mitigación de las vulnerabilidades encontradas posterior al análisis?

1.3. OBJETIVO GENERAL.

Plantear una metodología para el análisis de vulnerabilidades de software encontradas en servidores de una red mediante el uso de herramientas de Software Libre.

1.4. OBJETIVOS ESPECÍFICOS.

- Identificar el procedimiento para garantizar un análisis de vulnerabilidades satisfactorio dentro de los límites planteados.
- Determinar que servidores de la red empresarial se encuentran con una mayor probabilidad de ser atacados debido a sus vulnerabilidades de software.
- Establecer las mejores herramientas para el análisis de vulnerabilidades de software de servidores dentro de la red empresarial.
- Proponer soluciones viables para la mitigación de las vulnerabilidades de software encontradas en los servidores de una empresa.

1.5. ANTECEDENTES.

En la actualidad, la mayoría de las empresas cuentan con servidores dentro de su red, los cuales son los encargados de proporcionar los diferentes servicios que requiere la empresa, razón por la cuál es requerido que el nivel de seguridad existente en los sistemas informáticos se encuentre muy alto con la finalidad de garantizar la tanto la protección de la información que se maneja por parte de las empresas como la disponibilidad de los servicios que se entregan al equipo corporativo.

La virtualización de servidores es ahora uno de los procesos más importantes para introducir innovaciones y nuevas tecnologías en el mundo del trabajo. Estos sistemas incluyen virtualización de memoria, redes y administración de carga para los dispositivos. Se utiliza para facilitar la virtualización de los sistemas informáticos y en muchos casos para mejorar el rendimiento y un uso más eficiente de los recursos del servidor promoviendo la disponibilidad, la recuperación y la descentralización de servicios de administración. (Doña, García, López, Pascual y Pascual, 2010, p.1)

Tener una infraestructura con hardware físico en pequeñas y medianas empresas que cuentan con una infraestructura de red con servidores ya no es viable en la actualidad puesto que presenta inconvenientes cuando hablamos de aumento de prestaciones de hardware ya que el costo para actualización de piezas de hardware para mejorar el rendimiento de los diferentes sistemas informáticos es muy elevado, además, esto implica que para adquirir hardware físico para una empresa se requiere sobredimensionarlo con la finalidad de mantener operativa siempre a la empresa. La virtualización permite una actualización de componentes de una manera mucho más sencilla ya que el hardware de un sistema informático virtualizado es escalable.

Sin embargo, no solo es cuestión de hardware, es importante la parte de software, que es el encargado de proporcionar los diferentes servicios que se manejan las empresas; en este aspecto

dentro de pequeñas y medianas empresas no existe un grado alto de seguridad informática para los servidores de la red empresarial y esto se debe a la falta de monitoreo de vulnerabilidades que se puedan presentar dentro de los sistemas informáticos.

En esta época se ha tratado con mayor rigurosidad los análisis de vulnerabilidades mediante prevenciones o revisiones de software mediante metodologías planteadas por varios autores en trabajos de investigación como, por ejemplo, el proceso investigativo para una "Metodología de Análisis de Vulnerabilidades para Pequeñas y Medianas Empresas" de la Pontificia Universidad Javeriana, Bogotá, Colombia, la cual propone un proceso para un análisis de vulnerabilidades no únicamente para sistemas informáticos, sino también trata de cubrir cualquier tipo de vulnerabilidad que pueda presentarse en la empresa.

Si bien no existe una metodología estándar como tal, que indique el procedimiento a seguir para un análisis de vulnerabilidades de sistemas informáticos, se puede seguir como guía la metodología propuesta por Ángel Arias en su trabajo de tesis "Análisis de vulnerabilidades de servidores virtuales, caso práctico servicios web informativos de la ESPOCH". En este trabajo se proporciona información de cómo realizar el análisis respectivo al servidor de servicios web de la Universidad Superior Politécnica de Chimborazo mediante una metodología propuesta por el autor.

Pero, en este caso el trabajo a realizado pretende usar herramientas de Software Libre para facilitar la identificación de vulnerabilidades, así como su respectivo análisis, ampliando el estudio no a un único servidor, sino a los servidores que comúnmente se encuentran en una red.

1.6. ALCANCE.

El trabajo de titulación tuvo su inicio con la virtualización de los servidores para el caso de estudio, los cuales fueron configurados para entregar servicios que comúnmente se manejan dentro de una red empresarial; para conseguir simular una red de servidores se procedió con el uso de GNS3 que permite el diseño de una topología de red. Se excluyó el resto de los equipos que se encuentran dentro a la red tales como: switches, routers, Firewalls, entre otros. Se trabajó con una cantidad de 3 servidores virtualizados pues se consideraron

Se continuó con una revisión de diferentes herramientas de Software Libre que se emplearon para la investigación de vulnerabilidades de software que puedan presentarse en los servidores de la red empresarial planteada; se seleccionaron 3 herramientas las cuales se consideraron óptimas para el propósito del trabajo. Posteriormente se planteó una metodología para la identificación y análisis de vulnerabilidades de software.

El presente trabajo se considera por concluido con la entrega de resultados y la guía metodológica que incluye la observación de los resultados obtenidos para llevar a cabo un correcto análisis de vulnerabilidades de software para servidores virtualizados de una red empresarial.

1.7. METODOLOGÍA.

Se utilizó una metodología investigativa para llevar a cabo el desarrollo del trabajo, puesto que el enfoque tiene a la búsqueda de las razones o causas del problema que se ha planteado, definiendo el cómo han sucedido las situaciones presentadas o el porqué de las situaciones que ocurrieron.

El presente trabajo partió desde la implementación de sistemas de información como son servidores en un ambiente virtualizado, si bien no existe una metodología estándar para una virtualización completa, se basará en las buenas prácticas para una correcta virtualización en la cual se toman en consideración los recursos de hardware asignados para los servicios que se ofrecerán, así como la configuración adecuada de los equipos para finalmente verificar su funcionamiento mediante las pruebas de funcionamiento para los servicios que fueron configurados.

Se consideraron varias herramientas de Software Libre para la realización del análisis a efectuado; las herramientas seleccionadas fueron aquellas que cumplieron con los requerimientos para garantizar la cobertura de vulnerabilidades de software que puedan presentarse dentro de los servidores de la red. Las herramientas fueron descritas acerca de cómo es su funcionamiento mas no se consideró el análisis interno de la herramienta, es decir, se centró únicamente en el uso de la herramienta para los fines pertinentes.

Para el análisis de vulnerabilidades de software se describió en detalle cómo se debe realizar la ejecución del plan para dicho análisis, así como las herramientas a utilizarse y las razones del porqué fueron seleccionadas dichas herramientas para llevar a cabo una ejecución eficiente del análisis de vulnerabilidades de software de los sistemas informáticos propuestos.

Se examinaron los resultados obtenidos presentando las posibles causas que dieron paso a las vulnerabilidades halladas con la finalidad de mejorar la seguridad de los sistemas informáticos con los que cuenta los modelos de empresas en análisis proponiendo soluciones viables para la reducción de vulnerabilidades de software dentro de la red.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2. MARCO TEÓRICO.

2.1. Máquinas Virtuales.

Se define a una máquina virtual (VM) como un sistema informático (ordenador, servidor) que se encuentra virtualizado y ejecutado sobre un software conocido como hipervisor el cual es el encargado de la asignación de los recursos a las máquinas virtuales. Estas máquinas funcionan independientemente una de otra y cada una puede tener su propio sistema operativo y su propia asignación de recursos como: memoria, CPU, almacenamiento, etc.

2.2. Hipervisores.

VMware define a un hipervisor como un proceso el cual permite la creación y ejecución de máquinas virtuales, es decir, se considera como monitor de máquinas virtuales. (VMware, 2022)

Rd Hat menciona que gracias a los hipervisores es posible la distribución de los recursos físicos con los que cuenta el sistema host hacia las máquinas virtuales que se encuentran montadas sobre este. (Red Hat, 2022)

El hipervisor quien separa la parte física del ambiente virtual, por ende, también es el encargado de la gestión de la programación de los recursos de las máquinas virtuales para que el hardware físico ejecute las operaciones o instrucciones que solicitan las máquinas virtuales. A los hipervisores se los puede separar en 2 tipos:

- Bare Metal o Tipo 1: Estos se encargan de comunicarse con los recursos físicos directamente. Por ejemplo:
    - VMware: ESXi, vSphere
    - Microsoft: Hyper-V

    - Red Hat: KVM
    - Citrix: XEN
    - IBM: Power VM
- Alojados o Tipo 2: Este tipo de hipervisores funcionan como una aplicación más dentro del ordenador host. Por ejemplo:
    - VMware: WorkStation
    - Oracle: VirtualBox

2.3. Virtualización.

La virtualización es una técnica que permite ejecutar varias máquinas virtuales con todas sus características (tanto de hardware como: memoria, procesador, almacenamiento, etc. Como de software como es el caso del sistema operativo que se usará) sobre un hardware físico con la finalidad de hacer valer toda la capacidad de procesamiento y rendimiento de los recursos disponibles. La virtualización hace uso de software el cual permite la imitación de las características de hardware para la creación del sistema virtualizado.

Las máquinas que se encuentran funcionando dentro del entorno virtualizado desempeñan funciones de manera independiente una de otra, es decir, se encuentran aisladas de las demás permitiendo que cada máquina virtual funcione como un equipo físico, pese a encontrarse todos estos dentro de una misma infraestructura de hardware.

Uno de los mayores beneficios de la virtualización es que nos permite distribuir los recursos un equipo físico hacia las máquinas virtuales (VM) logrando así aprovechar toda la capacidad de procesamiento del equipo, así como la reducción de costos al no requerir mayor cantidad de infraestructura física. Adicionalmente, VMware afirma que gracias a la virtualización es posible aumentar tanto la escalabilidad de la infraestructura TI como la flexibilidad y rendimiento de esta. (VMware, 2022)

La virtualización puede considerarse una opción viable para las empresas puesto que:

> *“Esto permite a las organizaciones particionar un equipo o servidor físico en varias máquinas virtuales. Cada máquina virtual puede interactuar de forma independiente y ejecutar sistemas operativos o aplicaciones diferentes mientras comparten los recursos de una sola máquina host.” (Microsoft, 2022).*

Es importante tener en consideración que, si bien la virtualización saca el máximo provecho de un servidor físico, las máquinas virtuales que se encuentren alojas dentro de este tendrán un rendimiento levemente menor al de su host. Además, si bien las VMs trabajan de manera independiente unas de otras, todas son dependientes de la infraestructura o servidor físico sobre el cual se encuentren levantados, por lo que, si llega a fallar o desconectarse la máquina física, todo el sistema virtualizado fallará.

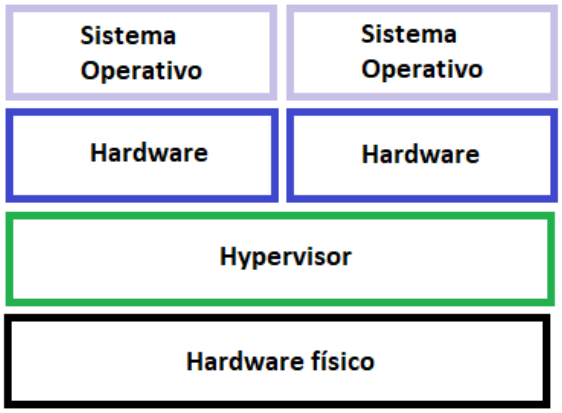
2.3.1. Tipos de Virtualización.

Se puede clasificar a la virtualización de máquinas virtuales de la siguiente manera:

- Virtualización de Hardware.
    - Esta virtualización permite que el hipervisor trabaje directamente sobre el hardware físico, es decir, para las máquinas virtuales los recursos que se les asignaron son de su uso exclusivo y no se comparte con otra máquina virtual. El hipervisor es quien transforma el hardware físico en hardware virtual para dividir virtualmente la capacidad del hardware físico para las máquinas virtuales que se monten sobre él cuando virtualicen sistemas operativos.

Figura 1

Estructura de la virtualización de Hardware

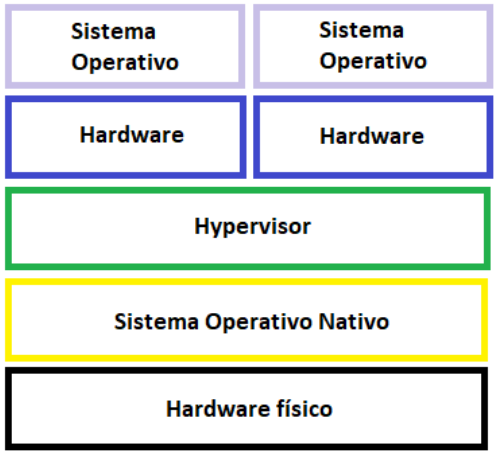


- Virtualización de Sistemas Operativos.
    - Para virtualizar sistemas operativos, se parte de un servidor que cuenta tanto con hardware físico como un sistema operativo, para posteriormente usar un hipervisor para crear instancias o máquinas virtuales sobre el servidor físico. Cada una de estas máquinas cuenta con su propio sistema operativo y funciona de manera independiente y aislada de las otras máquinas. Gracias a este tipo de

virtualización es posible utilizar los componentes de hardware de un modo óptimo y eficiente.

Figura 2

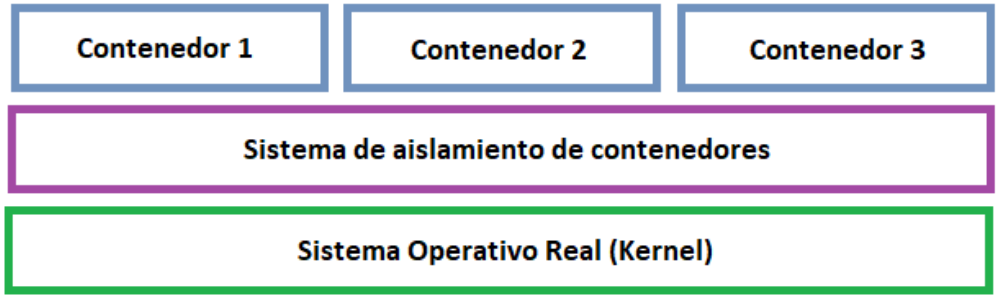
Estructura de la virtualización de Sistemas Operativos



- Virtualización a Nivel de Sistema Operativo.
    - El hardware físico cuanta con un sistema operativo en el cual se crean las instancias, particiones o contenedores, los cuales se encuentran aislados entre sí. Cada instancia es una réplica del sistema operativo host. Todo esto es posible gracias al Kernel del Sistema Operativo.

Figura 3

Estructura de la virtualización a nivel de Sistema Operativo



2.3.2. Enfoques de Virtualización.

- **Virtualización Completa.**
    - Ejecuta aplicaciones sobre esta base, de modo que el sistema alojado no tiene acceso al hardware físico del sistema anfitrión. Las soluciones de software más conocidas de este tipo de virtualización son Oracle VM VirtualBox, Parallels Workstation, VMware Workstation, Microsoft Hyper-V
    - Las máquinas virtuales poseen su propio entorno de hardware, el cual fue asignado por el hipervisor para poder ejecutar las aplicaciones sobre estos recursos, de esta manera la máquina virtual no tiene acceso al hardware físico del ordenador host. Las máquinas virtuales no saben que son virtualizados. Los hipervisores que permiten este enfoque de virtualización son (entre otros):
        - Hyper-V.
        - Oracle VirtualBox.
        - VMware WorkStation.
- **Paravirtualización.**
    - La paravirtualización es una técnica que permite que el software que se ejecuta en un sistema virtual haga operaciones en el hardware físico y omita la interfaz virtual para realizar dichas operaciones. La máquina virtual sabe que se está virtualizando.
    - Un sistema operativo invitado se modifica antes de instalarlo en una máquina virtual (VM) para que todos los sistemas operativos invitados del sistema puedan compartir recursos y trabajar juntos con éxito, en lugar de emular un entorno de hardware completo.

2.4. Infraestructura de redes.

Para que pueda existir tanto comunicación como conexión entre todos los dispositivos de una empresa se requiere una infraestructura de red, la cual está compuesta por aplicaciones de software como por quipos de hardware, como, por ejemplo: routers, servidores, firewalls, switches, entre otros.

Gracias a la infraestructura de red, es posible que los servicios que se manejan dentro de la red puedan comunicarse correcta y efectivamente tanto con usuarios como con los dispositivos pertenecientes a la misma. Por esta razón, es indispensable que una empresa u organización cuente con una infraestructura adecuada ya que de este modo se puede prevenir inconvenientes relacionados con la seguridad de los equipos informáticos.

2.5. Seguridad de la Información.

La seguridad de la información se basa en que la información representa un valor muy importante y un descuido en su manejo puede ser letal para las empresas. Contiene actividades para la gestión de la información, así como la garantía de confidencialidad e integridad de la información.

La información que se debe mantener segura dentro una empresa se puede identificar por los siguientes elementos:

- **Crítica:** Información requerida de alto grado, la cual se considera el motor de la organización.
- **Valiosa:** Información de muy alto valor de la cual depende el futuro de la empresa
- **Sensible:** información que podría poner en riego a la empresa frente a la competencia.

Cabe señalar ciertos elementos que deben responder a los objetivos de la seguridad de la información:

- **Confidencialidad:** Los datos y la información perteneciente a la empresa deben mantenerse únicamente dentro de la empresa y no debe ser difundidas a personal no autorizado.
- **Disponibilidad:** Refiere a posibilidad de que la información se encuentre disponible para ser accedida en cualquier momento por el personal de la organización.
- **Integridad:** La información no debe ser manipulada, ni alterada por ninguna razón; se debe garantizar que es auténtica.
- **Autenticación:** Permite identificar si la persona que está buscando acceder a la información coincide con los datos que proporciona para permitirle el acceso.

2.6. Vulnerabilidades de los Sistemas de Información.

Se define a una vulnerabilidad como una debilidad que pone en riesgo la seguridad de un sistema de información; en gran medida, los ataques hacia sistemas informáticos se deben a estas debilidades, que incluso pueden ser muy pequeñas, pero, el simple hecho de su existencia amenaza a la información de la empresa, la cual que se encuentra alojada en estos equipos informáticos.

Dentro de las posibles causas para que se puedan presentar vulnerabilidades pueden deberse a:

- Deficiente configuración de los equipos.
- Errónea gestión de acceso a información.
- Insuficientes o nulas políticas de seguridad.
- Errores de codificación de software.
- Mal uso de los sistemas informáticos.

- Puertas traseras presentes en los sistemas.
- Vulnerabilidad “0 days”.
- Factor humano.

Arévalo-Cordovilla et al. 2020, alegan que “En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones” p.836. Partiendo de esta premisa, podemos considerar que el activo más importante que tiene una empresa es la información que posee, razón por la cual es el activo al que debemos dar prioridad respecto a la seguridad ya que el giro de negocio de una empresa está basado en la información que poseen.

2.6.1. Tipos de Vulnerabilidades.

Las vulnerabilidades de software de los sistemas informáticos se pueden clasificar de la siguiente manera:

- **Desbordamiento de buffer:** La cantidad de datos que entran en un programa o aplicación supera la capacidad del buffer provocando la reescritura del contenido sobrante sobre el contenido original.
- **Condición de carrera (race condition):** Un recurso compartido es accedido por varios usuarios a la vez, provocando que el resultado de la operación dependa del orden de llegada de la petición del servicio.
- **Error de formato de cadena (format string bugs):** Se produce cuando no existe un control en el formato del ingreso de datos.
- **Cross Site Scripting (XSS):** Consiste en la ejecución de scripts dentro de páginas web cuya finalidad es el phishing para el robo de credenciales.

- **Inyección SQL:** Consiste en la inyección de código SQL malicioso para provocar fallas del motor de base de datos.
- **DOS:** Da como resultado que los usuarios no puedan acceder a un servicio, ya que este se encuentra caído debido a la sobrecarga de peticiones realizadas.
- **Ventanas Engañosas (Window Spoofing):** Ventanas que generalmente se encuentran en navegadores con la finalidad de que un usuario "clickee" en dicha ventana engañosa o fraudulenta para proporcionar su información y de este modo poder realizar un ataque.

2.7. Software Libre.

Se define como el software al cual los usuarios pueden acceder, modificar para mejorar o para beneficio propio, así como se debe poder copiar y distribuir el mismo. GNU menciona que el Software Libre es una cuestión de libertad, no de precio. (GNU, 2022)

Para que se pueda considerar un programa como software libre, debe seguir los liberales:

- El programa puede ser ejecutado con cualquier propósito que el usuario desee.
- El código fuente debe poder ser visible para todos y debe ser posible la modificación del software.
- Se debe poder realizar copias para su redistribución en beneficio de la comunidad.
- Debe ser posible realizar copias a versiones de software ya modificadas, permitiendo a la comunidad obtener los mismos beneficios e implementar otros.

2.8. Software Open Source

El software Open Source o de Código Abierto es desarrollado por la comunidad, ya que es posible tener acceso al código, por lo cual se facilita la revisión y mejora del software. Programadores pueden modificar el aplicativo y cobrar por dicha modificación, pero con un costo

inferior al de software propietario ya que la comunidad es la que generalmente cuenta con la versión base del programa.

Red Hat adule que:

> *“El movimiento de código abierto utiliza los valores y el modelo de producción descentralizado del software de código abierto para encontrar nuevas formas de resolver problemas en sus comunidades e industrias”.* (Red Hat, 2022)

CAPÍTULO III: SERVIDORES Y REDES

3. Servidores dentro de la red.

3.1. VirtualBox vs VMware.

En el capítulo anterior mencionamos que existen 2 tipos de hipervisores: los de tipo 1 o “Bare Metal” que son aquellos que son instalados directamente sobre el hardware físico y los de tipo 2 o alojados que son aquellos que se instalan sobre un sistema operativo local.

Si bien los hipervisores “Bare Metal” son empleados en su mayoría donde existen ambientes empresariales grandes por su usabilidad e interacción con el hardware, se utilizó para este trabajo un hipervisor alojado puesto que para el caso de estudio se consideraron tanto el alcance del proyecto como las limitaciones de hardware presentes para la implementación del mismo. Dentro de los hipervisores tipo 2, que generalmente son aquellos que se ejecutan sobre computadores personales o pequeños servidores, destacan 2 paquetes de software de virtualización por sus características, prestaciones y rendimiento: Virtual Box y VMware.

3.1.1. VirtualBox.

Nació como software privado bajo la mano de Innotek GmbH en 2007, luego, en 2008 Sun Microsystems pasó a ser propietario de Innotek GmbH y finalmente en 2010 Oracle Corporation adquirió Sun Microsystems cambiando el nombre a Oracle VM VirtualBox.

Permite una virtualización a nivel de sistema operativo que se encarga de realizar una virtualización completa para arquitecturas x86 y x64 de servidores y escritorios. Es una distribución gratuita de código abierto bajo la licencia GLP V2.

Oracle VM VirtualBox permite la creación y ejecución de máquinas virtuales sobre el sistema operativo anfitrión, aislando las máquinas virtuales de la máquina física, sin embargo, hay un paquete de extensión que permite la interacción del entorno virtual con la máquina anfitrión.

Los sistemas operativos en los cuales se puede ejecutar este software son:

- Windows,
- GNU/Linux,
- macOS,
- Solaris.

3.1.2. VMware.

Es un software de virtualización de la empresa EMC Corporation. El software de VMware cuenta con una gran variedad de productos para la virtualización, desde software básico como VMware para virtualización y ejecución de máquinas virtuales hasta VMware vSphere que destaca como solución para la virtualización de Data Centers.

VMware al tener una gran cantidad de productos, cuenta con los 2 tipos de hipervisores que fueron mencionados previamente. Nos centramos en los productos de software de tipo 2 o también llamados alojados teniendo como base las limitaciones de hardware para implementar la virtualización de los servidores, adicionalmente, la comparativa que se utilizó para seleccionar el hipervisor óptimo para este caso de estudio requiere que los hipervisores pertenezcan al mismo tipo.

Estos hipervisores cuentan tanto con versiones de paga como de versiones gratuitas, todo dependerá del enfoque del uso que se le quiera dar, así como de las características que se requiera para el proyecto que se quiera llevar a producción.

Los sistemas operativos sobre los cuales se puede ejecutar este software son:

- Windows,
- GNU/Linux.

Si se desea ejecutar VMware sobre entornos Mac OS se requiere de la instalación de VMware Fusion, ya que el software de VMware de tipo 2 no está pensado directamente para trabajar sobre macOS.

3.1.2.1. VMware Workstation Player.

Esta distribución de software contiene tanto una versión gratuita, la cual se enfoca para uso personal o educativo, como una versión de paga la cual se enfoca para entornos comerciales y con una reducción de restricciones de uso y de características en comparación a su versión gratuita

3.1.2.2. VMware Workstation Player Pro.

VMware Workstation Pro proporciona una mayor cantidad de funcionalidades las cuales resultan muy útiles cuando se habla de entornos empresariales o para proyectos que requieren más características o prestaciones por parte del hipervisor. Entre las características que se pueden encontrar dentro de VMware Wirkstation Player Pro y no en su versión normal, tenemos:

- Generar Snapshots y clonar una máquina virtual desde el Snapshot.
- Compartir y replicar una máquina virtual
- Ejecutar sincrónicamente varias máquinas virtuales.

Workstation Player Pro, cuenta únicamente con versión con licencia y las características diferenciales anteriormente mencionadas fueron descritas con base en la versión de paga de Workstation Player.

3.1.3. Comparativa: Oracle VM VirtualBox y VMware Workstation Player.

Empezamos a realizar un análisis en primer lugar con los diferentes costos de los productos de cada hipervisor de tipo 2, con la finalidad de discernir los softwares potencialmente utilizables de los que no pueden ser viables.

Tabla 1

Lista de costos de licencias.

Hipervisor	**Costo**
Oracle VM VirtualBox	$ 0
Oracle VM VirtualBox Enterprise (Socket)	$ 930
VMware WorkStation Player (Uso personal/educativo)	$ 0
VMware WorkStation Player	$ 149.99
VMware WorkStation Player Pro	$ 199.00

Al momento de seleccionar sobre qué hipervisor se trabajará es importante realizar el análisis de costos, razón por la cual la decisión de decantarse uno sobre el otro puede deberse en gran medida al factor económico; como se puede observar en la tabla de costo de licencias, tanto VMware como VirtualBox cuentan con versiones de paga así como de versiones gratuitas; teniendo en consideración que las versiones de paga (Enterprise para Oracle y Workstation Player para VMware) son dedicadas al ambiente empresarial comercial , se omitieron para este caso de estudio puesto que, como se detalló en capítulos anteriores, el trabajo está limitado por las capacidades económicas y de hardware con las que se cuenta para llevar a cabo el proyecto.

No obstante, para la realización de la virtualización de los servidores se puede observar que ambos hipervisores comparados cuentan con la versión gratuita, la cual puede ser implementada

para el caso práctico, por esta razón, se deberán analizar otros factores como es el caso de rendimiento entre la máquina host con las máquinas virtuales de cada hipervisor.

Tabla 2

Comparativa de características generales.

Característica	VirtualBox	VMware
Tipo de Virtualización	Software y Hardware	Hardware
Sistemas Operativos sobre los que trabaja	Microsoft, Linux, macOS, Solaris.	Microsoft, Linux, macOS (mediante VMware Fusion).
Snapshots	Si permite guardar el estado de la máquina virtual.	Si es posible realizar snapshots únicamente en las versiones de paga.
Formato de Disco Virtual	VDI, VMDK, VHD, HDD.	VMDK.
Soporte de dispositivos USB	USB 2.0 y 3.0 mediante la extensión proporcionada por Oracle.	Soporta toda versión de dispositivos USB.
Tipo de adaptador de red	En puente, NAT, Host-Only, red NAT, red interna.	En puente, NAT, Host-Only.
Interfaz gráfica	Interfaz gráfica para el usuario.	Interfaz gráfica para el usuario.

Al analizar la tabla anterior, se puede observar que ambos hipervisores poseen similares características con diferencias que pueden ser factores decisivos para la selección de un hipervisor sobre otro.

Un punto importante que se analizó para la selección del hipervisor es la posibilidad de virtualización de software y hardware, si bien una virtualización de software permite emular por completo el sistema informático, tiene una gran desventaja frente a la virtualización de hardware que es un rendimiento menor. Tomando este aspecto en consideración se descartó como factor crítico para la selección del hipervisor ya que se optó por la virtualización de hardware por el

rendimiento que ofrece además de que los servidores virtuales operarán directamente sobre el hardware físico, y ambas opciones comparadas poseen esta opción.

La compatibilidad sobre los diferentes sistemas operativos que se encuentran en el mercado si se consideró como un factor importante a tener en consideración para la selección de un software ya que es imprescindible que el software sea compatible de ser posible con los sistemas operativos para que la mayoría de los usuarios puedan acceder a este servicio. En este punto VirtualBox es posible montarlo sobre un entorno macOS mientras que en VMware se requiere el uso adicional de VMware Fusion para poder trabajar sobre entornos macOS y del mismo modo para poder montar entornos macOS ya que de forma nativa no es posible. Sin embargo, al existir esta solución, se analizó otro punto, el cual se consideró crítico ya que de este depende para poder guardar el estado actual de una máquina o servidor virtual.

La capacidad de poder generar clones o restauraciones de máquinas virtuales a partir de un guardado del estado de una máquina fue muy importante para la decantación del hipervisor con el cual se trabajó pues esta característica permite entre otras cosas guardar la configuración de una máquina virtual y poder usarla a nuestra conveniencia ya sea como un respaldo o para la creación de otra máquina virtual con las mismas características. No obstante, ambas opciones permiten la generación de Snapshots, con la diferencia que en VMware se deberá recurrir a la versión de paga para poder gozar de esta característica. Ya que se mencionó previamente los valores de las licencias de los hipervisores, se analizó si es viable costear una licencia a cambio de contar con esta característica y más funcionalidades por lo cual se requirió una evaluación del rendimiento de cada hipervisor con la finalidad de seleccionar el óptimo para el caso de estudio propuesto.

Para la evaluación de comparación de rendimiento entre los diferentes hipervisores presentes en el mercado, se ha tomado como referencia el trabajo de Đorđević (2022): “Comparison of type-

2 hypervisor performance on the example of VirtualBox, VMware Workstation player and MS Hyper-V". Basado en este trabajo se tomaron los resultados obtenidos luego se someter una máquina virtual a diferentes Benchmarks en los diferentes hipervisores analizados. Cabe mencionar que el hipervisor Hyper-V de Microsoft fue descartado para el propósito de este trabajo puesto que el nivel de dificultad de uso se incrementa considerablemente para usuarios que no están muy relacionados con el tema de virtualización o carecen de conocimiento informático, adicionalmente se presentan problemas como la coexistencia con otros hipervisores que se encuentren instalados en el ordenador donde se requiera realizar la virtualización así como la imposibilidad de usar este hipervisor si no se cuenta con la versión Professional de Microsoft, puesto que solo está disponible para esta versión.

Se ejecutaron los mismos programas para análisis de rendimiento sobre las máquinas virtuales con la finalidad de que los resultados tengan el mismo impacto sobre cada máquina con las mismas características, pero alojada en diferentes hipervisores.

Para el ambiente de prueba se tuvieron las siguientes características propuestas en la Tabla 3:

Tabla 3

Componentes de ordenador base.

Componentes	**Características**
Procesador	Intel i7-8750H 2.2 GHz
RAM	DDR4 16 GB
Caché	6 MB L3
Disco	500 GB Kingston M.2
Sistema Operativo	Windows 11 Home x64

La máquina virtual la cual se sometió a las pruebas de rendimiento contó con las siguientes especificaciones para todos los hipervisores sobre los cuales se realizaron las pruebas:

Tabla 4

Características máquina virtual.

Componentes	**Características**
Procesadores Virtuales	1 procesador
RAM	2 GB
Disco Virtual	60 GB
Sistema Operativo	CentOS 7

Para el análisis se utilizó la herramienta Filebench para la generación de una gran carga de trabajo para el sistema de archivos y de almacenamiento. Esta herramienta permite la modificación de cargas de trabajo dependiendo de las necesidades del usuario. Los parámetros evaluados para las cargas de trabajo fueron:

- Fileserver,
- Webserver,
- Varmail,
- Randomfileaccess.

Para la realización de las pruebas se evaluó con una máquina virtual y con 3 máquinas virtuales (mismas características) ejecutándose simultáneamente. Realizados los test en los diferentes hipervisores se obtuvieron los siguientes resultados:

Tabla 5

Resultados análisis "fileserver".

Fileserver	**1 máquina virtual**	**3 máquinas virtuales**
VMware Workstation Player	75,48 MB/s	55,64 MB/s
Oracle VM VirtualBox	43,02 MB/s	30,17 MB/s

Como se pudo observar, los resultados muestran que, al realizar una carga de trabajo compleja de escritura aleatoria y secuencial, VMware se muestra superior significativamente a VirtualBox tanto en la ejecución de una máquina virtual como 3 simultáneamente.

Tabla 6

Resultados análisis "webserver".

Webserver	**1 máquina virtual**	**3 máquinas virtuales**
VMware Workstation Player	87,84 MB/s	79,73 MB/s
Oracle VM VirtualBox	48,18 MB/s	39,27 MB/s

La carga de trabajo para "Webserver" se evidenció que VMware es significativamente superior a VirtualBox casi por el doble de velocidad de lectura de componentes aleatorios.

Tabla 7

Resultados análisis "varmail".

Varmail	**1 máquina virtual**	**3 máquinas virtuales**
VMware Workstation Player	46,98 MB/s	10,93 MB/s
Oracle VM VirtualBox	21,84 MB/s	19,71 MB/s

Dentro de Varmail los resultados indicaron que existe un desempeño poco eficiente por parte de Virtualbox para la lectura de componentes aleatorios, así como para gran cantidad de escritura de componentes sincrónicos escritos aleatoriamente.

Tabla 8

Resultados análisis "randomfileaccess".

Randomfileaccess	**1 máquina virtual**	**3 máquinas virtuales**
VMware Workstation Player	6286,81 MB/s	5963,12 MB/s
Oracle VM VirtualBox	60784,42 MB/s	57764,45 MB/s

La evaluación de lectura de componentes aleatorios y de escritura masiva asincrónica de componentes aleatorios se puede observar que VMware sigue siendo mínimamente superior a VirtualBox. Sin embargo, esta evaluación fue la más pareja que se pudo encontrar entre los 2 hipervisores analizados.

Como se pudo observar existen varias características que destacan un hipervisor sobre otro y viceversa; se evidenció que VirtualBox tiene un buen rendimiento y presenta buenas prestaciones y es una opción viable sobre la cual se puede implementar la virtualización completa de los servidores del caso de estudio generando resultados aceptables, posicionándose por encima de VMware Workstation Player en su versión gratuita al contar con características que se encuentran restringidas en esta por no emplear la versión de paga. Sin embargo, en el aprovechamiento de recursos, en el rendimiento con el hardware físico y en la capacidad operativa de la máquina virtual, según las gráficas presentadas previamente se observó que VMware Workstation Player Pro tiene mayor ventaja sobre VirtualBox y uno de los factores para que se presenten estas características puede deberse al mismo hecho de ser una versión de paga, ya que se presenta esta versión para ya un uso comercial, donde los usuarios demandan tanto el rendimiento como la capacidad de contar con funcionalidades que una versión gratuita no pueda ofrecer, y en este punto VMware ha sido superior.

Se llegó a la conclusión de optar VMware Workstation Pro para el levantamiento de los servidores para el cado de estudio por las razones expuestas previamente sobre el rendimiento del hipervisor, así como el comportamiento y optimización que tiene con el hardware del ordenador físico. Si bien VirtualBox es la opción más viable por las características que ofrece para su versión gratuita, se la descartó ya que se tuvo la oportunidad de trabajar con VMware Workstation Player Pro con licencia, la cual contiene mejores características y funcionalidades que VirtualBox.

3.2. Servidores dentro de la red.

Para que se pueda trabajar con los servidores es necesario que estos se encuentren dentro de la red empresarial; al haber trabajado en un ambiente virtual, se requirió el uso de GNS3 para la simulación de una red.

GNS3 es una herramienta de software de código abierto bajo la licencia GLPv3 que permite el diseño y simulación de una red con todos los equipos que esta cuenta. GNS3 permite la implementación de dispositivos físicos como virtuales para la red diseñada.

Para el presente trabajo se utilizó GNS3 para la implementación de la red, la cual se consideró únicamente los servidores como dispositivos de la red puesto que el objetivo del trabajo fue el análisis de vulnerabilidades de software de los servidores presentes en la empresa, razón por la cual no se contempló el resto de los equipos de los que se compone una red.

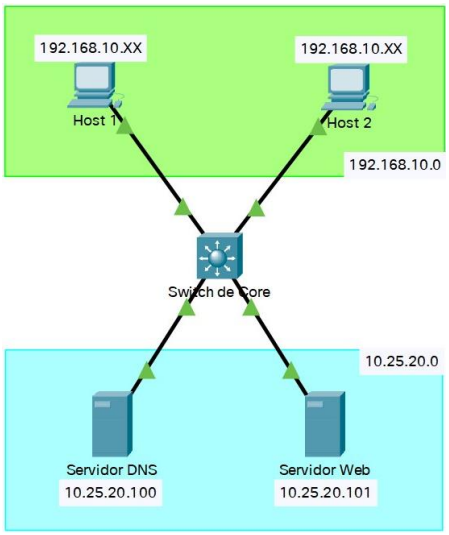
Se optó por la implementación de 2 servidores para la red: Servidor DNS y Servidor Web, los cuales fueron analizados en capítulos posteriores.

3.3. Topología de red.

La Figura 4 representa la composición de la red que se pueden encontrar dentro de las PYMES que cuentan con una infraestructura de red básica.

Figura 4

Topología de estrella de la red.



Se procedió a usar la topología de estrella puesto que es una de las topologías de las más sencillas para implementarlas en empresas pequeñas y medianas. Adicionalmente esta topología permite contener varias capas (capas de core, distribución y capas de acceso).

La topología de estrella permite que todos los dispositivos finales como ordenadores, tabletas o laptops se conecten a un nodo central como es el caso de los servidores que se identifican en la Figura anterior. Esta topología para las PYMES es una opción viable puesto que el nodo central es quien transfiere los datos que le llegan de un equipo hacia otros equipos destino.

Emplear esta topología permite que se puedan añadir equipos a la red de una manera más sencilla, puesto que al no conectarse con ningún otro dispositivo que sea el nodo principal, no requiere configuraciones adicionales. Además, en caso de que ocurra algún fallo o desconfiguración se lo puede solucionar fácilmente; la detección de fallas es mucho más sencillas por la configuración de la misma.

La red se segmento para separar los hosts de los proveedores de servicios para la red, para ello se utilizó un Switch de Core de capa 3 para la creación de VLANs donde se tiene:

- VLAN para hosts y
- VLAN para servidores.

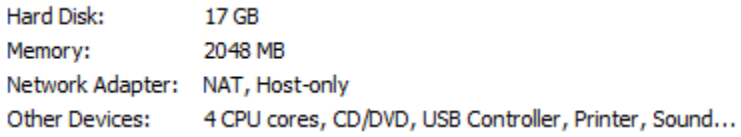
3.3.1. Servidor DNS.

El servidor de Sistema de Nombres de Dominio por sus siglas del inglés DNS es el encargado de darle un nombre a la dirección IP de una página web para poder acceder a ella de una manera más sencilla ya que no se deberá memorizar los números de dicha dirección. Del mismo modo, el servidor DNS se encarga de convertir el dominio de una página web en una dirección IP. Todos los dominios y direcciones IP de los sitios web son alojados en la base de datos de este servidor donde su tiempo de respuesta es inmediato ya que únicamente almacena esta información y no es una base de datos muy extensa.

Las características para el servidor DNS implementado fueron las siguientes:

Figura 5

Características de hardware: Servidor DNS.

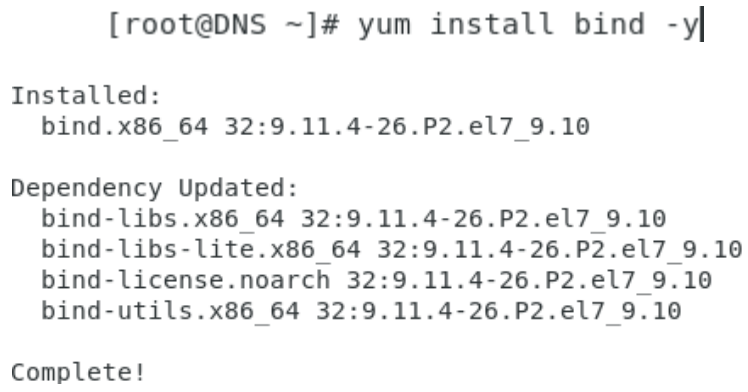


El levantamiento y algunas configuraciones esenciales del servidor se describen a continuación. Se utilizó la distribución de GNU/LINUX CentOS 7 para el servidor DNS con su respectiva configuración.

Se inició con la instalación de BIND, la cual es una herramienta de configuración del servicio de nombres de Dominio DNS

Figura 6

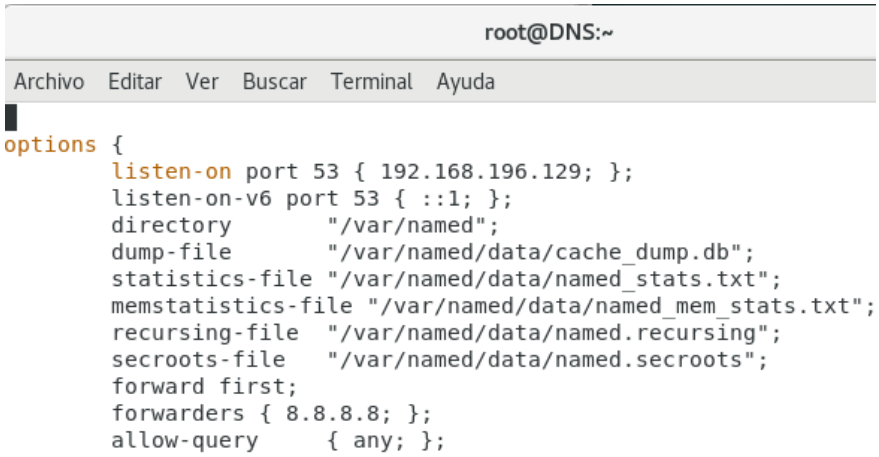
Instalación paquetes BIND.



Para la configuración del DNS se realizaron los siguientes cambios en el archivo que se detalló a continuación, teniendo como dirección IP la de nuestro Servidor

Figura 7

Modificación archivo named.conf.



Para la configuración de la zona directa que es igual a la de nuestro dominio, en este caso fue: *titulacion.com.* Se configuró de tipo maestro y el tipo de archivo se ha colocado: *sochi.titulacion.com* (este nombre puede ser cualquiera tanto para la zona directa o inversa).

Figura 8

Modificación zona directa en named.conf.

Para la zona inversa configuramos de la siguiente manera.

Figura 9

Modificación zona inversa en named.conf.

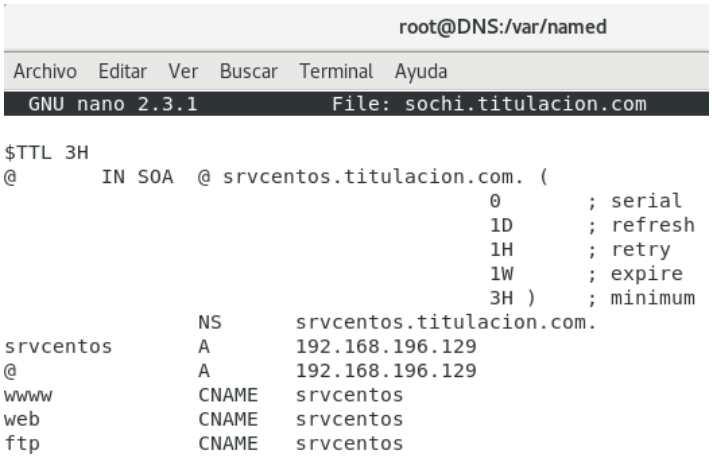
```
zone "196.168.192.in-addr.arpa" IN {
        type master;
        file "inversa.titulacion.com";
};
```

Guardada la configuración, se verificó que no exista ningún error en la configuración con el comando que se muestra a continuación: *named-checkconf /etc/named.conf*

Posteriormente copiamos el archivo que se encuentra en la carpeta hacia el nombre del archivo que creamos para la zona y procedemos a editar la configuración. Posteriormente se ingresó el FQDN que es el nombre de dominio totalmente calificado.

Figura 10

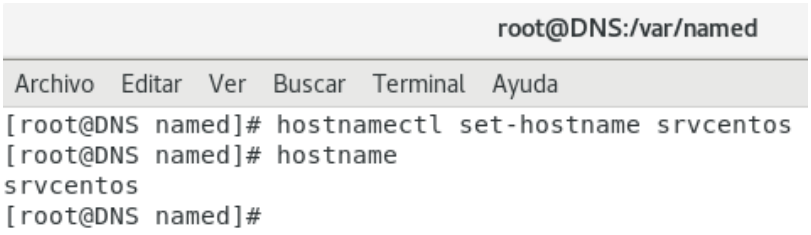
Modificación de archivo de zona directa.



Procedemos a cambiar el nombre del servidor.

Figura 11

Modificación del nombre del servidor.



Se copió el archivo de la zona directa a la zona inversa. Posteriormente se configuró la zona inversa.

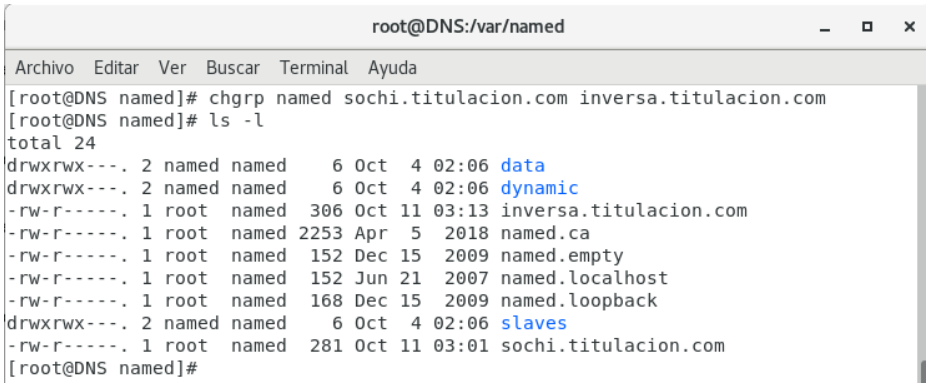
Figura 12

Modificación de archivo de zona inversa.

Realizados los cambios se procedió a cambiar el grupo de las zonas.

Figura 13

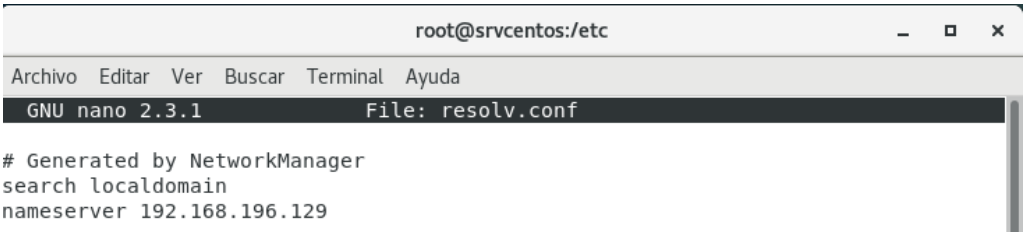
Cambios de los grupos de las zonas directa e inversa, de root a named.



Procedimos a editar el archivo *resolv.conf.*

Figura 14

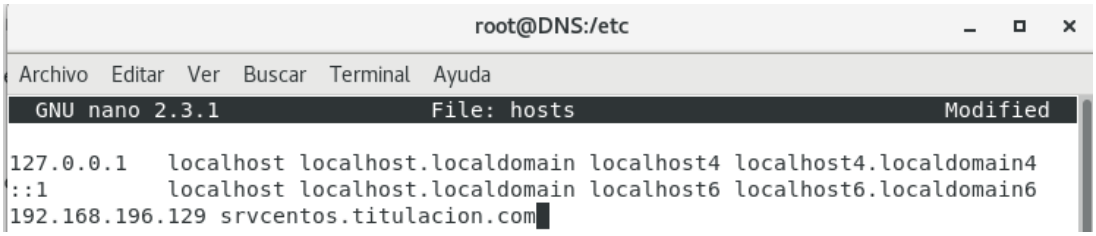
Modificación de la dirección del servidor DNS.



El archivo hosts también modificamos y se añadió el nombre del servidor.

Figura 15

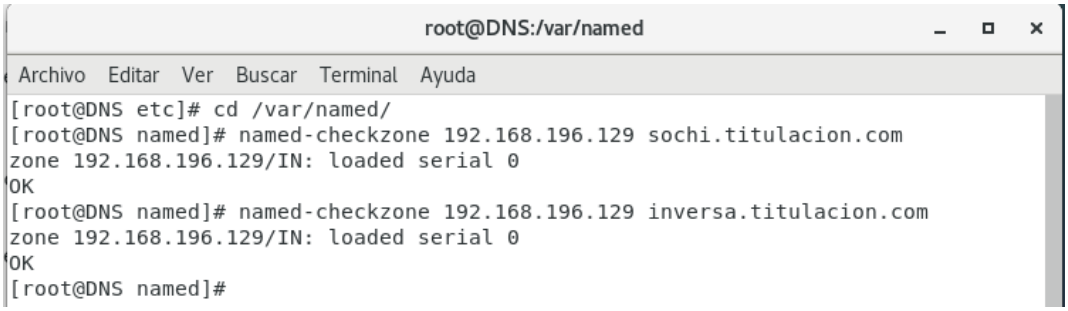
Archivo con dirección de servidor DNS.



Verificamos la configuración de la zona directa y de la inversa.

Figura 16

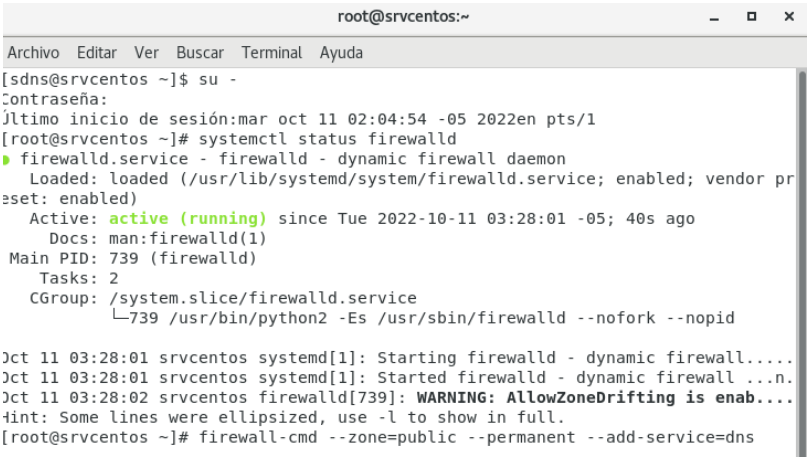
Revisión correcta configuración de ambas zonas.



Verificamos el estado del Firewall y modificamos las reglas del firewall para que los clientes puedan acceder.

Figura 17

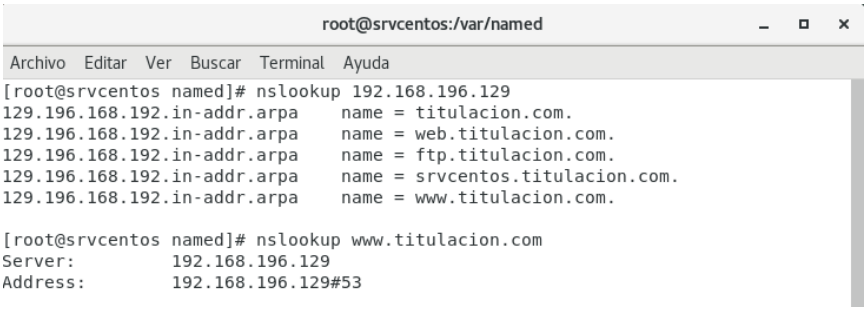
Estado del Firewall.



Para finalizar la configuración se inició el servicio de dominio DNS con el comando *systemctl start named.* Se puede realizar verificaciones que resolución de IP en dominio y viceversa.

Figura 18

Comprobación resolución de dominio e IP del servidor DNS



3.3.2. Servidor de Correo Electrónico.

El Servidor de Correo Electrónico es uno de los servidores comúnmente encontrados en las empresas puesto que es quien se encarga tanto de enviar como de recibir los correos electrónicos de quienes se encuentren utilizando sus servicios, como por ejemplo permite la comunicación entre usuarios que pertenezcan a la misma empresa.

Las características para el servidor de Correo Electrónico implementado fueron las siguientes:

Figura 19

Características de hardware: Servidor de Correo.

En primer lugar, se procedió a actualizar cualquier directorio del sistema operativo con apt-get update. Posteriormente descargamos iRedMail el cuál funcionará como nuestro servidor de correo electrónico de código abierto. iRedMail permite la administración de nuestro correo electrónico, así como la administración de usuarios.

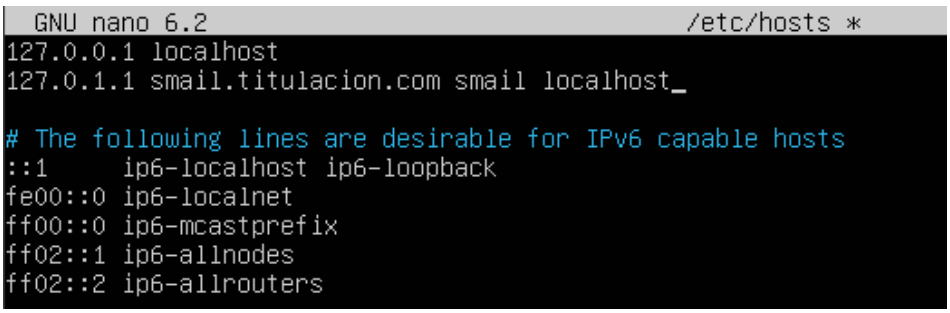
Figura 20

Actualización directorios SO y descarga de iRedMail.

Una vez completada la descarga se procedió a descomprimir el empaquetado y a otorgarle permisos para poder realizar las modificaciones respectivas. Luego se continuó con la configuración del nombre del dominio en el archivo *hosts*. Para este servidor se lo colocó el nombre de *smail.titulacion.com*.

Figura 21

Configuración del nombre de dominio del servidor.



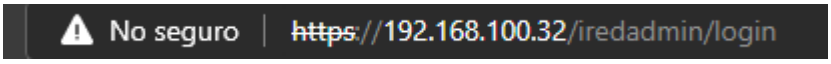
Se ejecutó el archivo iRedMail.sh para levantar el servicio de iRedMail. Finalizada la ejecución, se presenta una pantalla donde se realizan las configuraciones para el servidor. Dichas configuraciones fueron:

- Ubicación del directorio: /var/vmail
- Servidor web para ejecutar: Nginx
- Motor de Base de Datos: MariaDB
- Dominio de correo: correotitulacion.com

Terminada la instalación con el resto de las características por defecto procedimos a configurar el Firewall para poder acceder al servidor de correo. Al finalizar dicha configuración, con el comando *ifconfig* se visualiza la dirección IP de nuestro servidor para poder acceder desde nuestro navegador.

Figura 22

Dominio para acceder al servidor de correo electrónico como administrador.



Para el ingreso como administrador, se lo hace con el usuario *postmaster* y el dominio que especificamos (correotitulacion.com) en conjunto con nuestra contraseña.

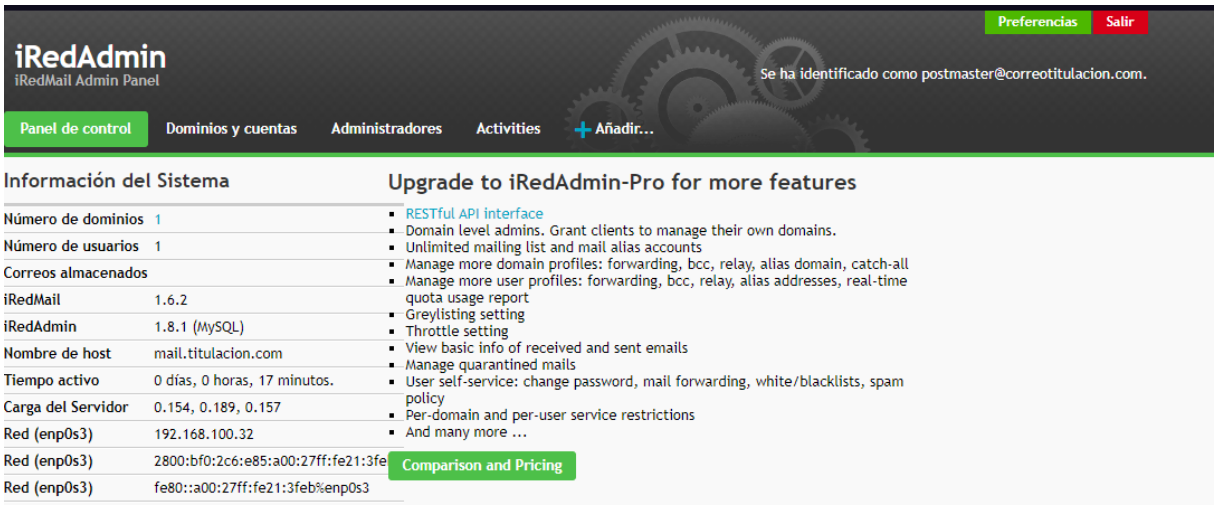
Figura 23

Inicio de sesión con usuario administrador.

Una vez iniciada sesión tenemos la interfaz de administrador en la cual se pueden crear usuarios de correo electrónico para la empresa.

Figura 24

Interfaz de administrador de iRedMail.



En los Anexos se puede revisar la creación de usuarios de correo electrónicos. Una vez creados los usuarios, nos podemos dirigir a la dirección del servidor para entrar como usuario y no como administrador.

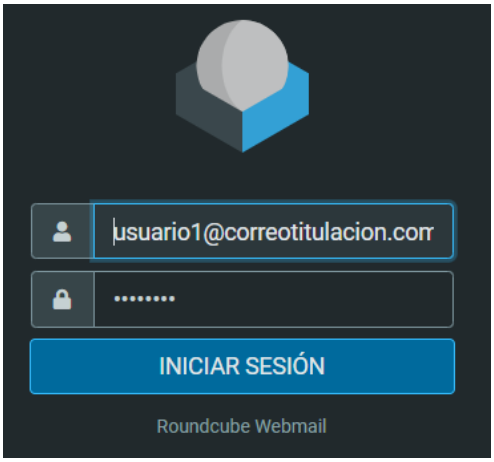
Figura 25

Dominio servidor de correo electrónico para usuarios.

Ingresado al dominio del servidor, se observa la interfaz para ingresar como usuario al correo electrónico de la empresa previamente configurado.

Figura 26

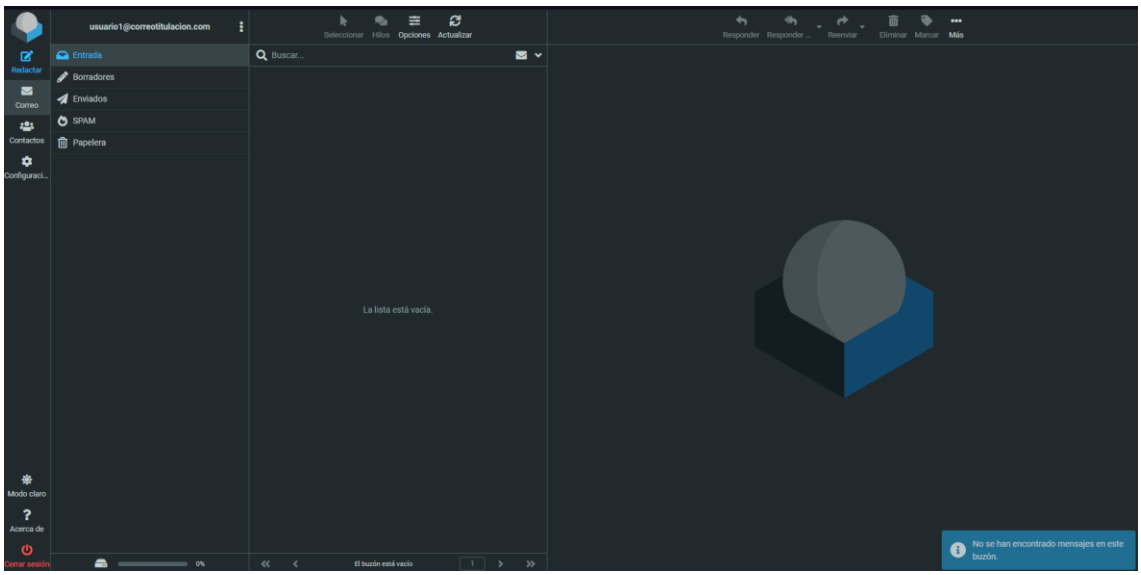
Interfaz de inicio de sesión de usuario normal de correo electrónico.



Una vez iniciado sesión ya podemos ver como se encuentra la interfaz de nuestro servidor correo para los usuarios de la empresa.

Figura 27

Interfaz de servicio de correo electrónico.



CAPÍTULO IV: HERRAMIENTAS PARA ANÁLISIS DE VULNERABILIDADES

4. Herramientas para análisis de vulnerabilidades de servidores.

En este capítulo se describieron las herramientas de Software Libre que se utilizaron para el respectivo análisis de vulnerabilidades. Para poder realizar el análisis se ocupó una máquina virtual con sistema operativo Kali Linux ya que este cuenta con una gran variedad de herramientas de distinto tipo.

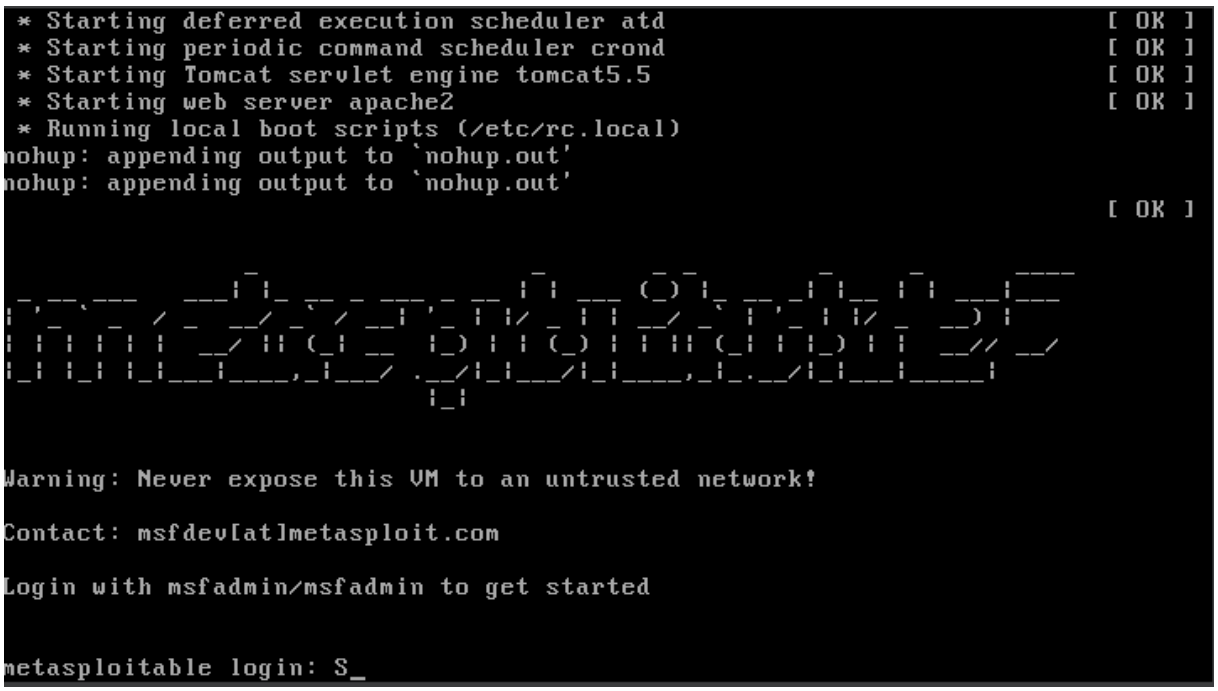
Adicionalmente se implementó un servidor llamado Metasploitable 2 el cual es un sistema que cuenta con todo tipo de vulnerabilidades como por ejemplo de: sistema operativo, configuración, redes, entre otras. Metasploitable 2 fue creado con la finalidad de probar todas las herramientas presentes en Kali, razón por la cual se lo ocupó con la finalidad de comparar las vulnerabilidades encontradas en un servidor vulnerable en contra de los servidores DNS y de correo electrónico que se encontraban configurados.

Para implementar el servidor Metasploitable 2, al ser Open Source lo debemos descargar de SourceForge como archivo comprimido. Descomprimimos el archivo y posteriormente procedemos a crear una máquina virtual con el nombre Metasploitable 2, de sistema operativo Linux con distribución de Ubuntu.

Las características que se debe añadir son de 1024 MB para memoria RAM y finalmente para almacenamiento seleccionamos disco virtual existente y seleccionamos el archivo que descomprimimos con extensión vmdk.

Figura 28

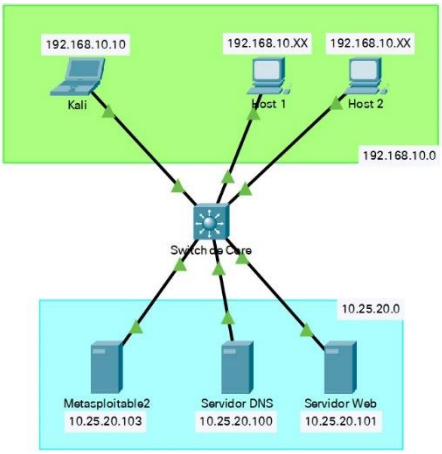
Servidor Metasploitable 2.



La red empresarial implementada tanto con el ordenador de Kali que fue el servidor encargado de identificar las vulnerabilidades de los servidores de la red empresarial del caso de estudio; así como con el servidor Metasploitable 2 el cual fue el servidor con el cuál se realizaron las comparaciones de las vulnerabilidades halladas en los servidores configurados, quedó de la siguiente manera:

Figura 29

Red empresarial completa con equipos para análisis



Las herramientas que se presentan a continuación son unas de las varias posibilidades de herramientas que existen de Software Libre para realizar un análisis de vulnerabilidades en los servidores.

4.1. NMAP.

NMAP es una herramienta de red de código abierto muy utilizada para el reconocimiento de sistemas y servicios, así como para la identificación de puertos abiertos y detección de sistemas operativos. NMAP es una herramienta muy versátil y poderosa que se puede utilizar de muchas maneras y con una gran variedad de opciones.

Utilizado para escanear los dispositivos que se encuentran en la red (servidores, celulares, etc.), prácticamente cualquier dispositivo que tenga una IP. Sin embargo, también se puede usar esta herramienta para identificar los servicios se encuentran en ejecución, así como la versión del servicio.

Esto es muy importante en especial para el propósito de este trabajo ya que con ello es posible elaborar un informe para la empresa sobre los servicios y sus versiones con la finalidad de conocer si se requiere algún tipo de actualización en los procesos debido a los fallos presentes en dicha versión, evitando así posibles vulnerabilidades dentro del sistema.

4.2. Naabu.

Es una herramienta que puede descargarse para el servidor Kali Linux, es muy similar a NMAP, puesto que sirve para el análisis de puertos enviando paquetes de tipo SYN. El escaneo rápido que realiza lo puede hacer de un host, así como de una lista de host y la respuesta que se muestra es de todos aquellos puertos que entregan una respuesta.

Proporciona menos información ya que únicamente presenta los puertos que se encuentran abiertos, mas no los servicios que se ejecutan sobre estos. Tiene menos comandos que pueden resultar útiles.

4.3. Nessus.

Es un programa de escaneo de vulnerabilidades, puede ser ejecutado por medio de comandos en la consola como por medio de una interfaz gráfica. Nessus al igual que otras herramientas, realiza un escaneo de los puertos, y para ello hace uso de la herramienta NMAP por su gran potencial y utilidad que representa, no obstante, Nessus cuenta con un propio software para analizar puertos, pero, no tan avanzado y rentable como NMAP.

Nessus cuenta con una versión de código abierto gratuita, la cual permite realizar un análisis básico al igual que la entrega de reporte de dicho análisis, y también posee una versión de paga la cual se caracteriza por el soporte que puede brindar, así como permitir un análisis mucho más completo

Esta herramienta es una buena opción por lo completa que es (en su versión licenciada), puesto que, posee una gran cobertura para la identificación de vulnerabilidades y fallos de seguridad que se puedan encontrar tanto dentro de los equipos informáticos como en las aplicaciones que estas manejan. Adicionalmente, esta herramienta al ser semi automática, permite planificar la hora en la que deseamos que se realice un análisis, así como el tipo de escaneo que se requiere.

4.4. Dimitry.

Esta herramienta de Software Libre es posible encontrarla en el repositorio de GitHub y es utilizada para reunir información como, por ejemplo: escanear los puertos que se encuentren abiertos de un servidor, identificar los subdominios que pueda tener un objetivo, adquirir información y detalles del servidor que tenga alojada una aplicación o página web en esta, entre otras.

Si bien esta herramienta contiene varias características que nos pueden resultar útiles como la obtención de direcciones de correo electrónico vinculadas al dominio del servidor objetivo o analizado; al realizar pruebas de uso, la información que entrega, lo hacen aplicaciones también y de una manera óptima, ya que, se pudo evidenciar que tarda más la entrega de resultados de esta aplicación en comparación, por ejemplo, de NMAP.

4.5. Nikto.

Nikto es una herramienta con la cual es posible realizar un escaneo de vulnerabilidades y entregar un reporte con los resultados encontrados. El análisis que realiza puede ser a la red como un sistema objetivo.

Las características que presenta Nikto es muy similar al resto de herramientas para el análisis de vulnerabilidades, sin embargo, si podemos destacar un aspecto de esta herramienta es el reporte

que esta genera ya que propone un reporte bastante detallado de los resultados que ha encontrado en el análisis realizado.

4.6. OpenVAS.

Es una herramienta de análisis de vulnerabilidades muy útil para encontrar fallos en la seguridad de los sistemas objetivos. Esta herramienta es muy completa y similar a Nessus, pero, con la diferencia que ésta si se mantuvo de licencia gratuita.

Identifica vulnerabilidades de los sistemas informáticos a través del análisis de puertos y otras pruebas programadas por OpenVAS. Es posible escanear la configuración de los sistemas e identificar los fallos de configuración; recopila información de los servicios en ejecución, escanea los puertos abiertos y las posibles vulnerabilidades de software que pueda presentar el equipo analizado.

La herramienta es posible utilizarla tanto en un equipo informático dentro de la red como en equipos de red externa, lo que da paso a la simulación de un ataque real.

Es posible configurar la herramienta para que se mantenga en un monitoreo constante para que pueda proporcionar alertas cuando se detecte algún fallo o vulnerabilidad. Adicionalmente, cuando se realiza un análisis, se emite un reporte completo con las vulnerabilidades y fallos encontrados.

4.7. OWASP-ZAP.

Es una herramienta para el análisis de vulnerabilidades la cual está basada en las buenas prácticas de seguridad; posee una interfaz gráfica. Identifica los fallos y vulnerabilidades, y las entrega en un reporte. Esta herramienta puede ser muy útil para la realización de auditorías informáticas para seguridad de los equipos informáticos, así como de la red.

Una notable diferencia de entre otras herramientas que tienen el mismo objetivo es que presenta posibles soluciones a las vulnerabilidades que ha encontrado. Es una herramienta bastante útil para páginas web que se encuentran alojadas en un servidor, puesto que, cuentan con varias opciones avanzadas para un análisis de esta.

4.8. Legion.

Es una herramienta de prueba de penetración de red semiautomático en el descubrimiento, reconocimiento y explotación de sistemas de información. Similar a NMAP. Hace escaneos automáticos mediante el uso de herramientas como NMAP y otras más herramientas para la recolección de información.

Gracias a la gran cantidad de servicios que ofrece, es posible realizar ataques de fuerza bruta y almacenar los resultados para generar informes de lo recolectado.

CAPÍTULO V: ANÁLISIS DE RESULTADOS

5. Selección de Herramientas para el Análisis de Vulnerabilidades.

Para el análisis de las vulnerabilidades de los servidores presentes en una red empresarial se han tomado en consideración las siguientes herramientas, las cuales fueron mencionadas en el capítulo anterior:

- NMAP,
- OpenVAS,
- OWASP-ZAP.

Se tomó la decisión de trabajar con estas herramientas ya que al poner en ejecución todas las herramientas que se mencionaron en el capítulo anterior, las 3 seleccionadas cumplen con las características necesarias para la finalidad buscada para este trabajo. Adicionalmente, podemos encontrar que ciertas funcionalidades de una herramienta se encuentran implementadas dentro de las herramientas seleccionadas o en su defecto poseen menos funcionalidades que una herramienta similar.

5.1. Comparativa de Herramientas.

Se procedió a realizar una comparación de las herramientas seleccionadas en contra de las descartadas con la finalidad de brindar un panorama más claro de la selección realizada para el trabajo en cuestión.

5.1.1. NMAP vs Naabu, Dimitry, Nikto.

Estas herramientas proporcionan información similar en cuanto a su enfoque al análisis de vulnerabilidades; Naabu proporciona menor información que NMAP, ya que lo único que esta nos indica es los puertos que se encuentran abiertos y los servicios asociados a dichos puertos.

Si hablamos de la herramienta Dimitry, caracterizamos que esta puede realizar una identificación de los subdominios de una aplicación o página web a diferencia de NMAP que no realiza dicha función, pues esta herramienta aparte de analizar los puertos de un equipo informático se enfoca a un análisis de servidores web, no obstante, NMAP brinda más información respecto al escaneo de puertos, así como de un mejor rendimiento que Dimitry. Si bien NMAP no posee las funcionalidades de identificar los subdominios de una página web, así como la obtención de los correos electrónicos asociados al servidor analizado, veremos que estas funcionalidades se encuentran presentes en las otras herramientas seleccionadas.

Nikto es otra aplicación con características similares, destacando sobre sus similares por su capacidad de proporcionar un reporte detallado sobre los resultados obtenidos de su escaneo de puertos (principal función), no obstante, al proporcionar más detalles del análisis y al tener más funcionalidades NMAP, se ha descartado esta aplicación ya que para la emisión de reportes del análisis se han considerado las herramientas tanto OpenVAS como OWASP—ZAP.

NMAP integra las funcionalidades del resto de herramientas comparadas en este punto. Se ha seleccionado esta herramienta ya que proporciona información adicional sobre el equipo que nos encontramos atacando, pues, esta herramienta realiza ataques más forzados para sacar la mayor cantidad de información que pueda representar una vulnerabilidad.

5.1.2. OpenVAS vs Nessus

En esta comparativa de herramientas se optó por OpenVAS directamente ya que Nessus si bien tiene una versión gratuita, es muy limitadas las funciones que se pueden emplear en comparación a OpenVAS, además, OpenVAS cuenta con un adicional de funcionalidades que permiten simular un ataque real para encontrar vulnerabilidades.

OpenVAS posee similares funcionalidades que la versión licenciada de Nessus. OpenVAS emite reportes detallados y también cuenta con una interfaz gráfica para poder realizar los análisis. Además, a esta ser una herramienta semi automática, es posible configurarla para poder que se encuentre en constante monitoreo y programar fechas para que se realice un análisis, lo que no es posible con la versión gratuita de Nessus.

5.1.3. OWASP-ZAP, OpenVAS vs Legion

OWASP-ZAP se basa en las buenas prácticas para mantener seguros los equipos informáticos, razón por la cual emplea funciones como NMAP al igual que Legion, además OWASP-ZAP no se limita únicamente a los servidores del caso de estudio, es posible utilizarlo para servidores web. Si bien Legion es una herramienta de penetración semiautomática, se ha descartado ya que OpenVAS (herramienta seleccionada) también tiene un enfoque automático y comparte las funcionalidades presentes en Legion.

5.2. Resultados de vulnerabilidades encontradas en los servidores con el uso de herramientas propuestas.

A continuación, se presentan los resultados obtenidos del análisis de vulnerabilidades por cada herramienta sobre los servidores implementados.

5.2.1. NMAP.

Para el uso de esta herramienta se utilizaron varias funcionalidades para recolectar la mayor cantidad de información y que se describen a continuación:

Detección de servicios y versiones: Realiza un escaneo de los puertos, su estado, su servicio y la versión del servicio que se encuentra ejecutando. Permite conocer mucho más sobre los puertos, brinda más información.

Detección del sistema operativo: Este tipo de comando es un tipo de ataque más agresivo puesto que se está forzando a que se identifique el sistema operativo que está ejecutando en el servidor analizado. Este ataque es fácilmente detectable ante un sistema de seguridad por lo abrupto que es el ataque.

Escáner completo de todos los puertos y redes: Proporciona información si hay alguna vulnerabilidad y un poco de información de la misma

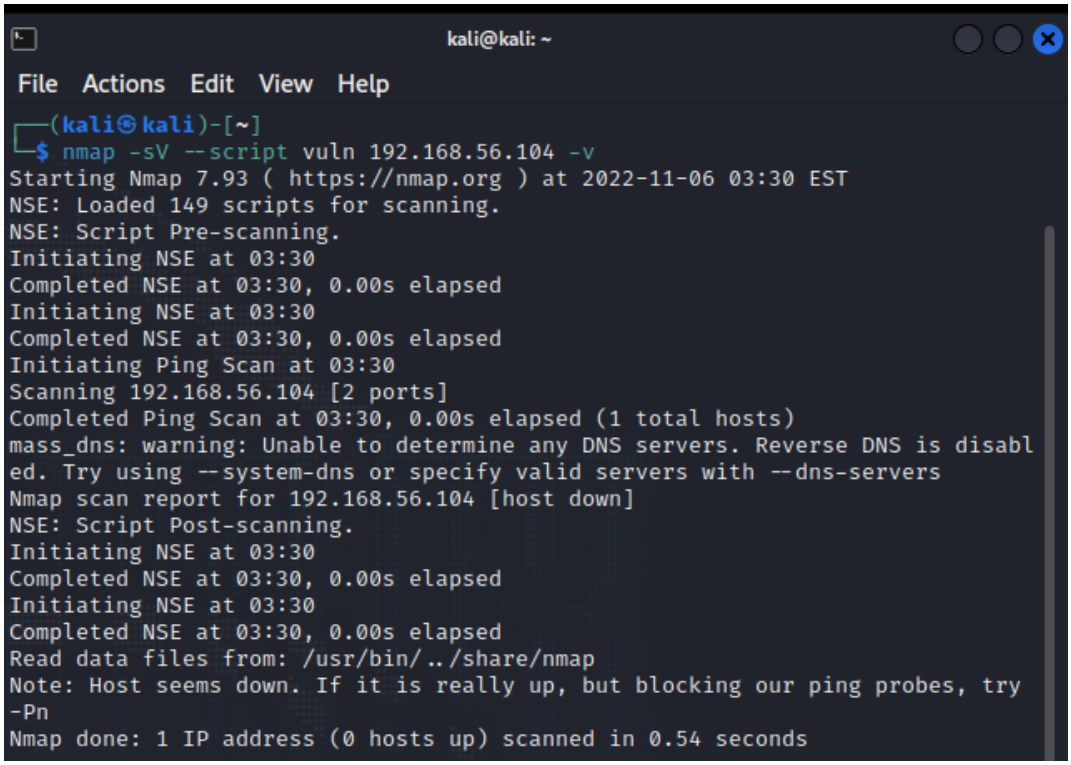
5.2.1.1. Servidor DNS y Servidor de Correo.

Servidor DNS

Detección de servicios y versiones: nmap -sV --script vuln dirección_IP -v

Figura 30

Ejecución herramienta NMAP al servidor DNS: Detección de servicios y versiones.

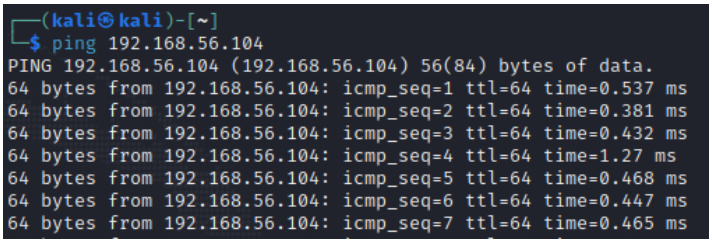


Al haber intentado realizar un escaneo de puertos hacia el Servidor DNS, no se pudieron obtener resultados debido a la configuración implementada en el equipo informático.

Se pudo evidenciar que posiblemente el host se encuentre apagado ya que no se pudo acceder ni enviar los paquetes para su respectivo análisis, sin embargo, como se puede apreciar en la Figura 31 que se muestra a continuación, el Servidor DNS se encuentra operativo.

Figura 31

Comunicación entre Servidor DNS y Máquina atacante (Kali).

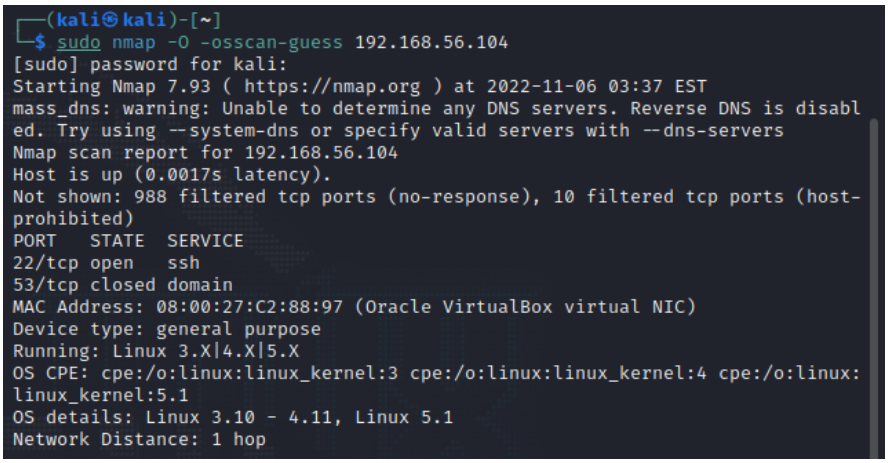


Por lo que se pudo concluir que la seguridad implementada no permite realizar un ataque forzoso ni evaluar los puertos abiertos dentro del servidor. Para solucionar esto se ocupó otras funcionalidades que entreguen los resultados esperados.

Detección del sistema operativo: nmap -O –osscan-guess dirección_IP

Figura 32

Ejecución herramienta NMAP al servidor DNS: Detección del sistema operativo.

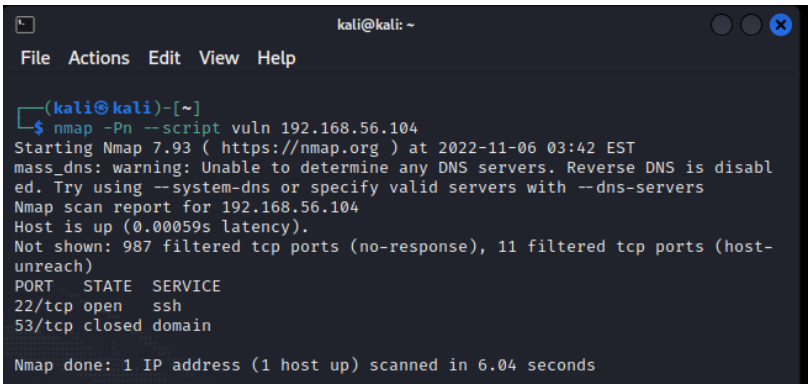


Como se observó en los resultados encontrados con el comando ejecutado, nos proporciona el sistema operativo que se encuentra corriendo en el Servidor DNS y ciertos detalles del sistema operativo como la versión; adicionalmente, se encontró ciertos servicios pertenecientes a puertos abiertos como es el puerto 22 del servicio SSH configurado para conexión remota con el servidor.

Escáner completo de todos los puertos y redes: nmap -Pn –script vuln dirección_IP

Figura 33

Ejecución herramienta NMAP al servidor DNS: Escáner completo de todos los puertos y redes.



Al ejecutar el comando que busca los puertos abiertos y las vulnerabilidades posibles dentro del Servidor DNS mediante el uso de scripts, los resultados arrojados indicaron que posee una configuración robusta el servidor puesto que las únicas vulnerabilidades que se encuentran se debieron al puerto 22 del servicio SSH que puede cerrarse en caso de no requerir conexión con el servidor de manera remota.

Servidor de Correo

Detección de servicios y versiones: nmap -sV --script vuln dirección_IP -v

Figura 34

Ejecución herramienta NMAP al servidor de Correo: Detección de servicios y versiones (1/2).

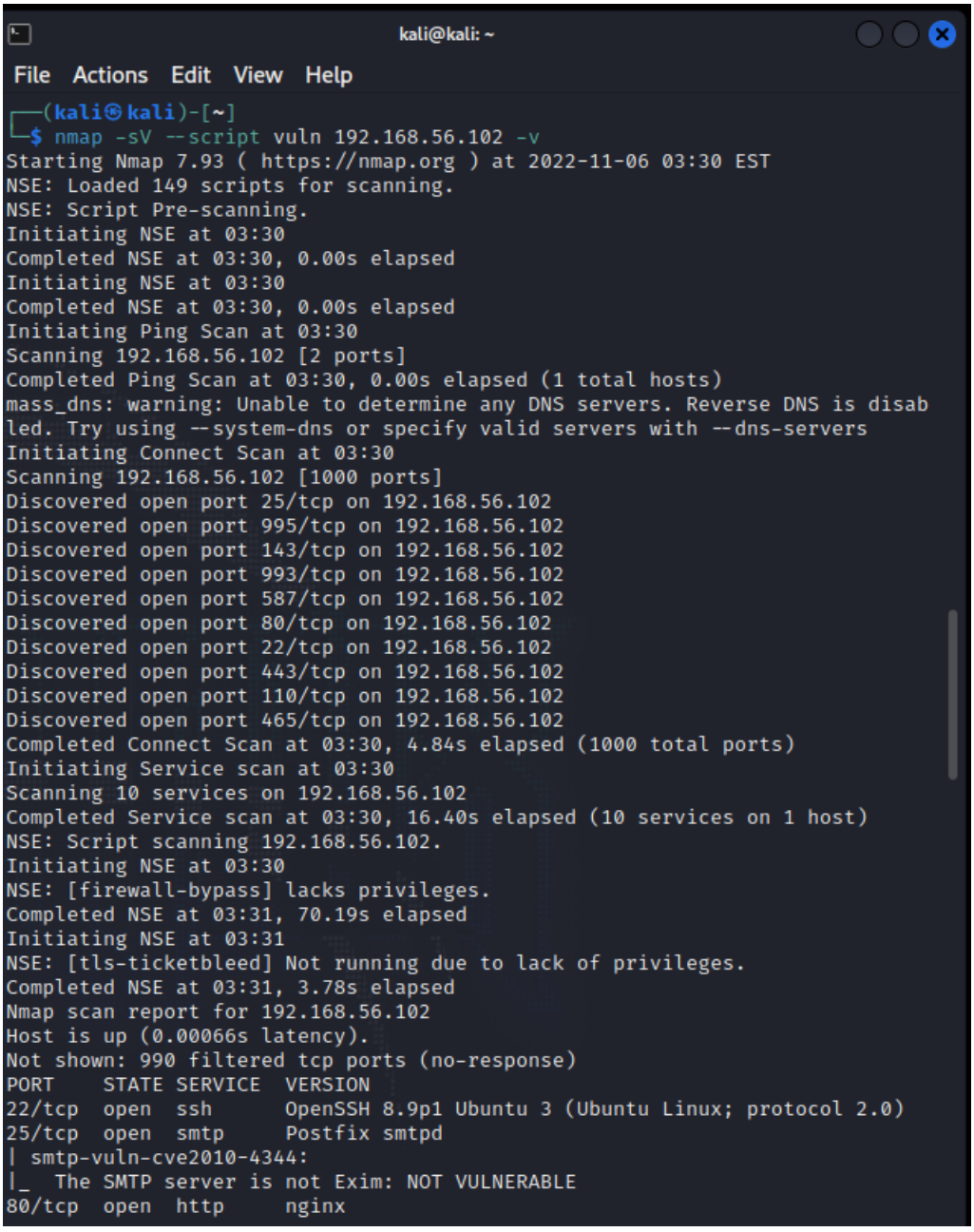


Figura 35

Ejecución herramienta NMAP al servidor de Correo: Detección de servicios y versiones (2/2).

A diferencia del servidor DNS, en la ejecución del comando de puertos y servicios, se encontraron varios puertos abiertos, pero, no todos ellos representan una vulnerabilidad ya que como podemos los puertos asociados a los servicios: SMTP, SSL, POP3, IMAPS, no representan puntos de vulnerabilidad. Sin embargo, al ser un servidor de correo, como nos señalaron los

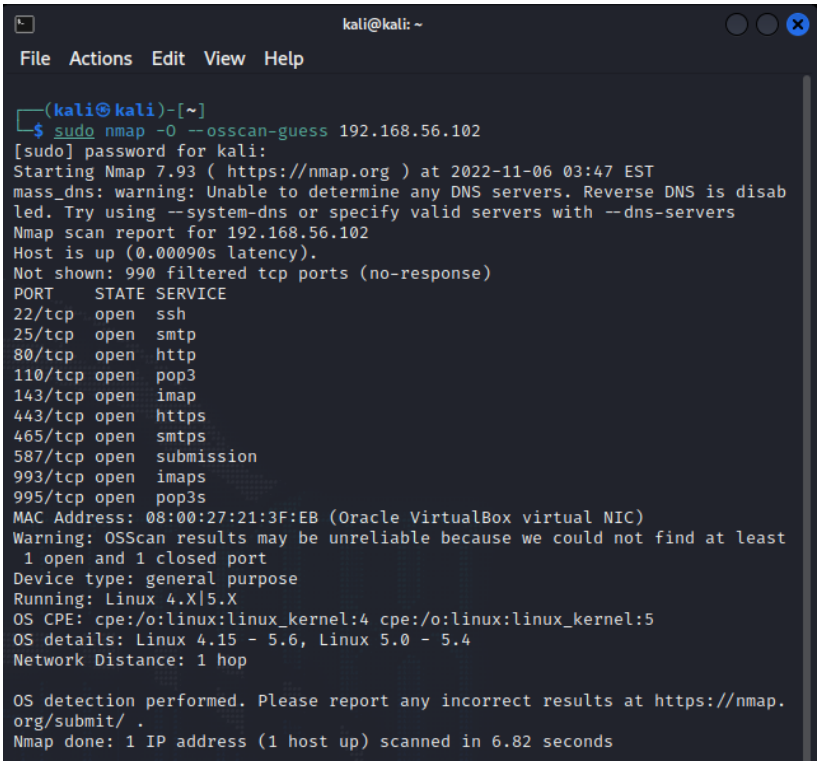
resultados, es posible que se presente una vulnerabilidad que puede ser explotada para realizar un ataque de denegación de servicio debido al servicio web del servidor de Apache que tiene implementado el Servidor de Correo.

Ubuntu Server es un sistema robusto por lo cual maneja protocolos de seguridad incluso para conexión SSH seguros. La solución óptima para evitar ataques de DoS (Denegación de Servicio) para nuestro servidor de correo electrónico comprende la configuración adecuada para el uso del correo únicamente para los miembros dentro de la red y la configuración de acceso hacia la red por parte de los equipos de seguridad de la red como los Firewall.

Detección del sistema operativo: nmap -O –osscan-guess dirección_IP

Figura 36

Ejecución herramienta NMAP al servidor de Correo: Detección del sistema operativo.

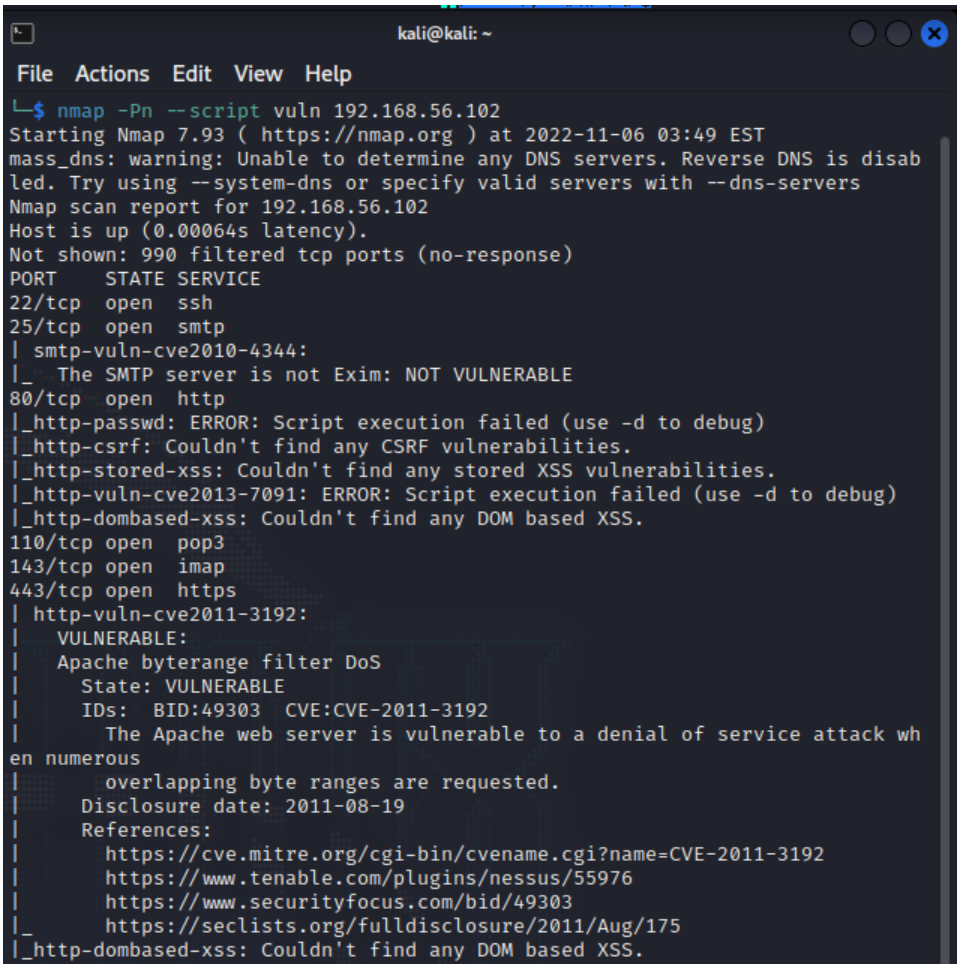


Del mismo modo que el comando ejecutado anteriormente, se pudo observar resumidamente los puertos que se encuentran abiertos, así como el sistema operativo que posee nuestro servidor y ciertos detalles de este.

Escáner completo de todos los puertos y redes: nmap -Pn –script vuln dirección_IP

Figura 37

Ejecución herramienta NMAP al servidor de Correo: Escáner completo de todos los puertos y redes.



Al ejecutar el comando que permite el escaneo de vulnerabilidades por medio de un script pudimos hallar la misma información sobre los puertos abiertos y si representan o no una

vulnerabilidad; adicionalmente, este script realizó un análisis más profundo ingresando a carpetas de archivos y servicios para verificar su configuración. Los resultados arrojados son los mismos ya analizados por comandos anteriores ejecutados.

5.2.1.2. Servidor Metasploitable2.

Detección de servicios y versiones: nmap -sV dirección_IP → nmap -sV --script vuln dirección_IP -v

Figura 38

Ejecución herramienta NMAP al servidor vulnerable: Detección de servicios y versiones (1/4).

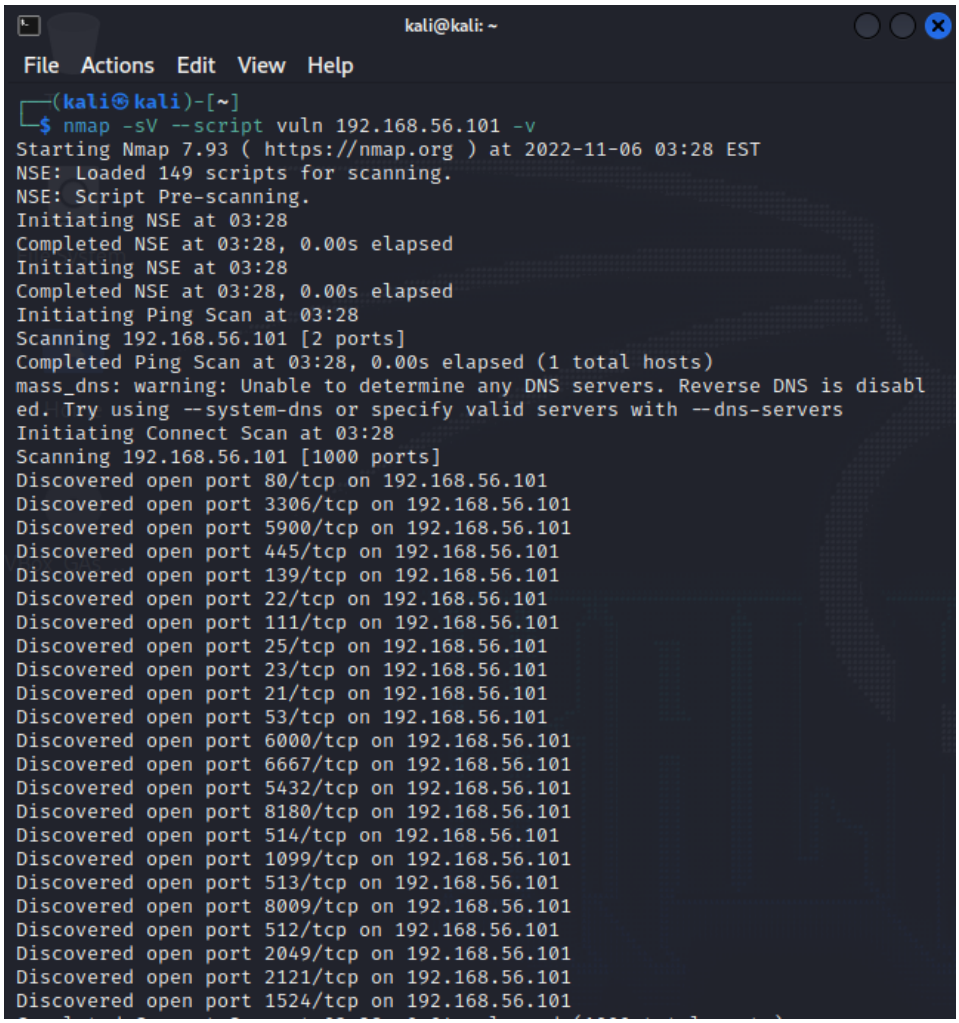


Figura 39

Ejecución herramienta NMAP al servidor vulnerable: Detección de servicios y versiones (2/4).

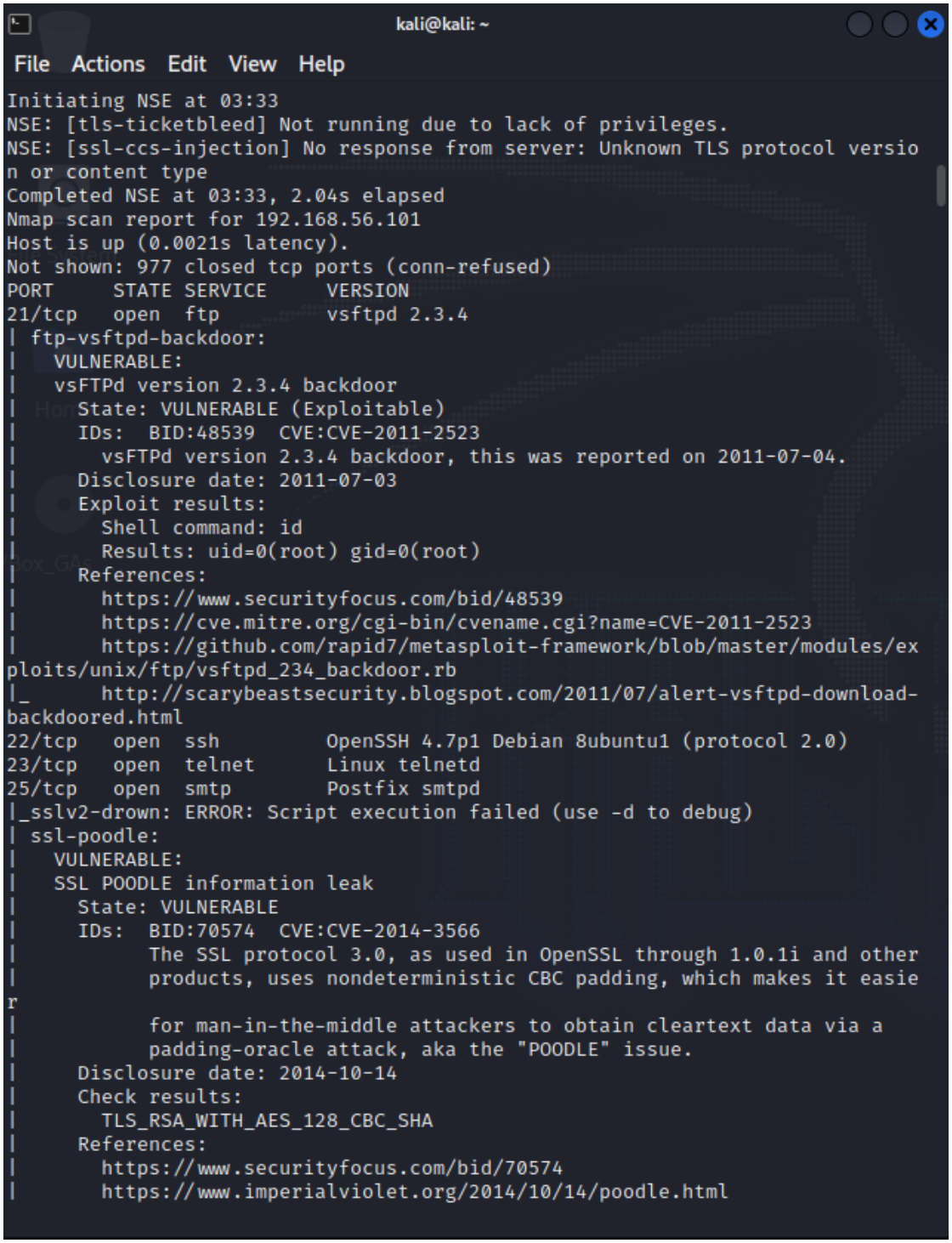


Figura 40

Ejecución herramienta NMAP al servidor vulnerable: Detección de servicios y versiones (3/4).

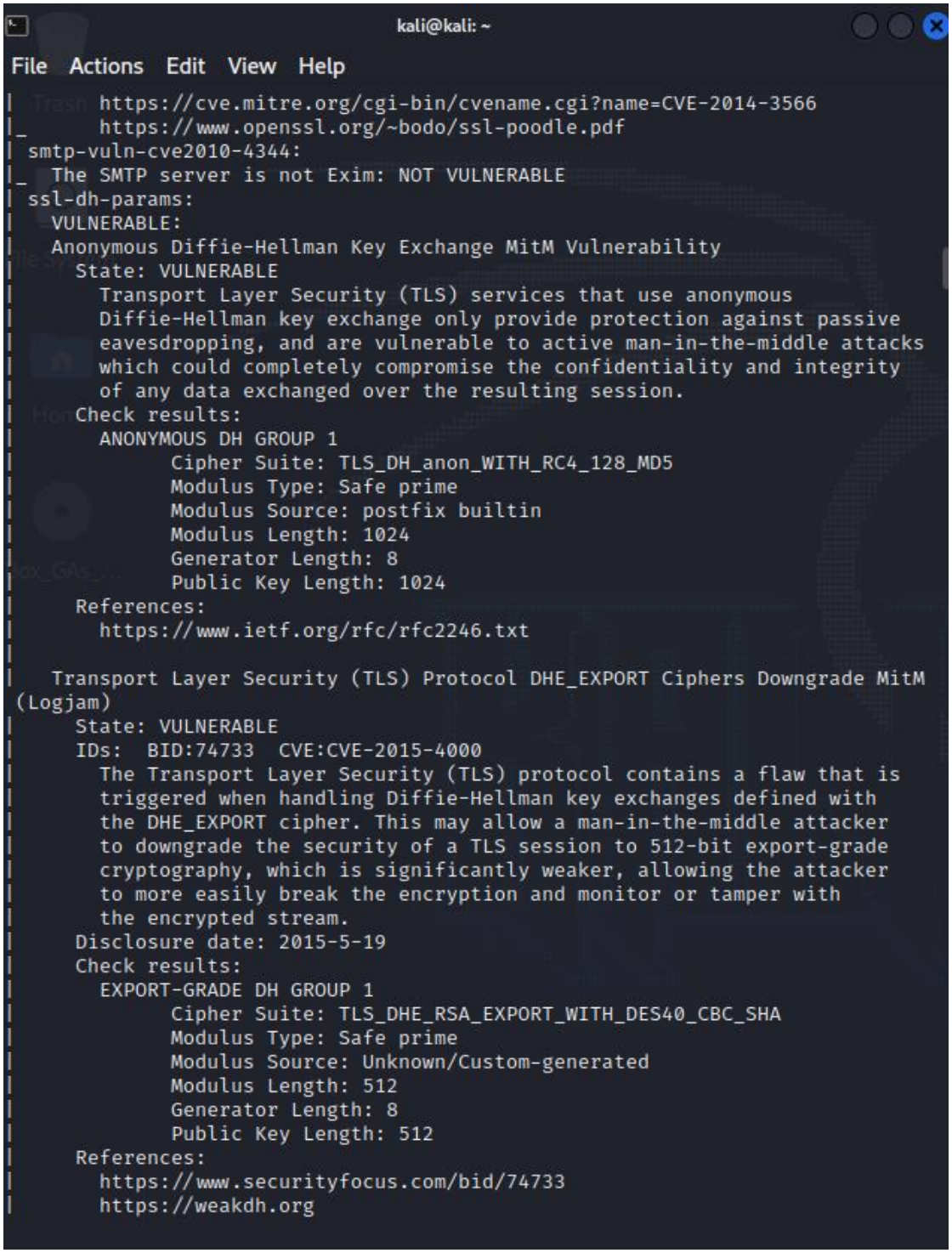
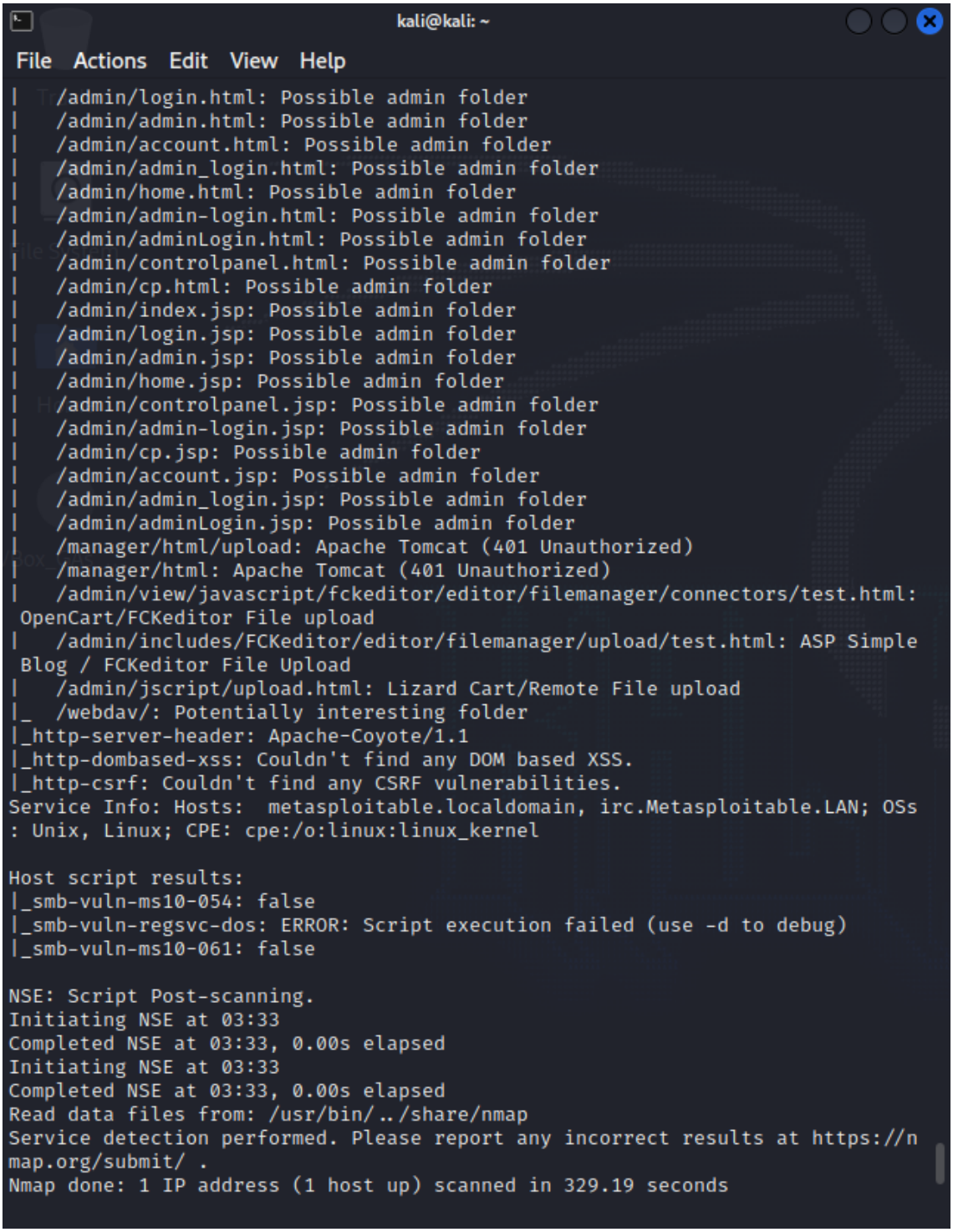


Figura 41

Ejecución herramienta NMAP al servidor vulnerable: Detección de servicios y versiones (4/4).



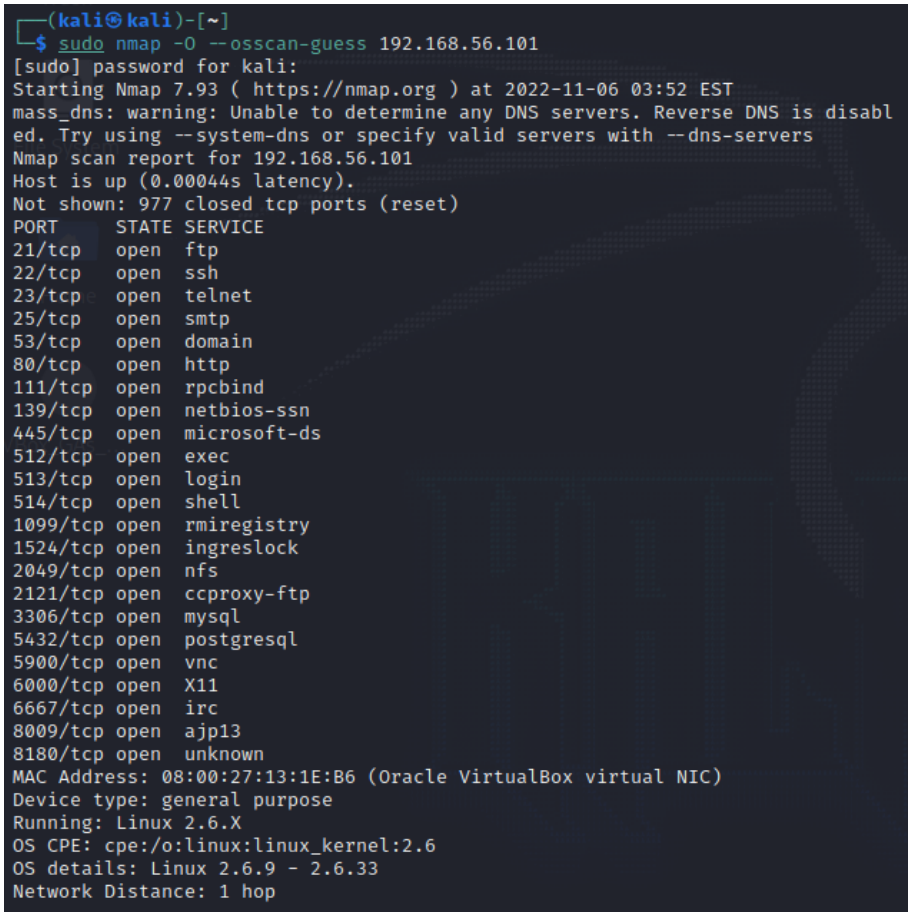
En el servidor vulnerable pudimos encontrar una gran cantidad de puertos abiertos y varios aspectos interesantes como es el caso de tener habilitados los servicios de SSH y Telnet, los cuales son usados para permitir conexiones remotas, sin embargo, cabe mencionar que Telnet es un tipo de comunicación por la cual se transfieren los datos en texto plano por lo cual es muy vulnerable y poco recomendable la utilización de este servicio, por lo cual, si hubiésemos encontrado este servicio ejecutándose en alguno de nuestros servidores de la red, deberíamos cerrar dicho puerto y reemplazarlo por un servicio de comunicación más segura como SSH.

Se observó adicionalmente que en su mayoría los puertos abiertos, los cuales se encuentran asociados a un tipo de servicio, son vulnerables debido a su configuración deficiente puesto que el objetivo de este servidor es ser atacado mediante la explotación de sus vulnerabilidades.

Detección del sistema operativo: nmap -O –osscan-guess dirección_IP

Figura 42

Ejecución herramienta NMAP al servidor vulnerable: Detección del sistema operativo.



Los resultados del sistema operativo detectado son correctos al igual que sus detalles. Se hizo mucho énfasis en el puerto 8180 que se encuentra abierto y se desconoce el servicio que este ejecuta ya que esto representa una puerta trasera abierta la cual es fácilmente explotable.

Escáner completo de todos los puertos y redes: nmap -Pn –script vuln dirección_IP

Figura 43

Ejecución herramienta NMAP al servidor vulnerable: Escáner completo de todos los puertos y redes (1/3).

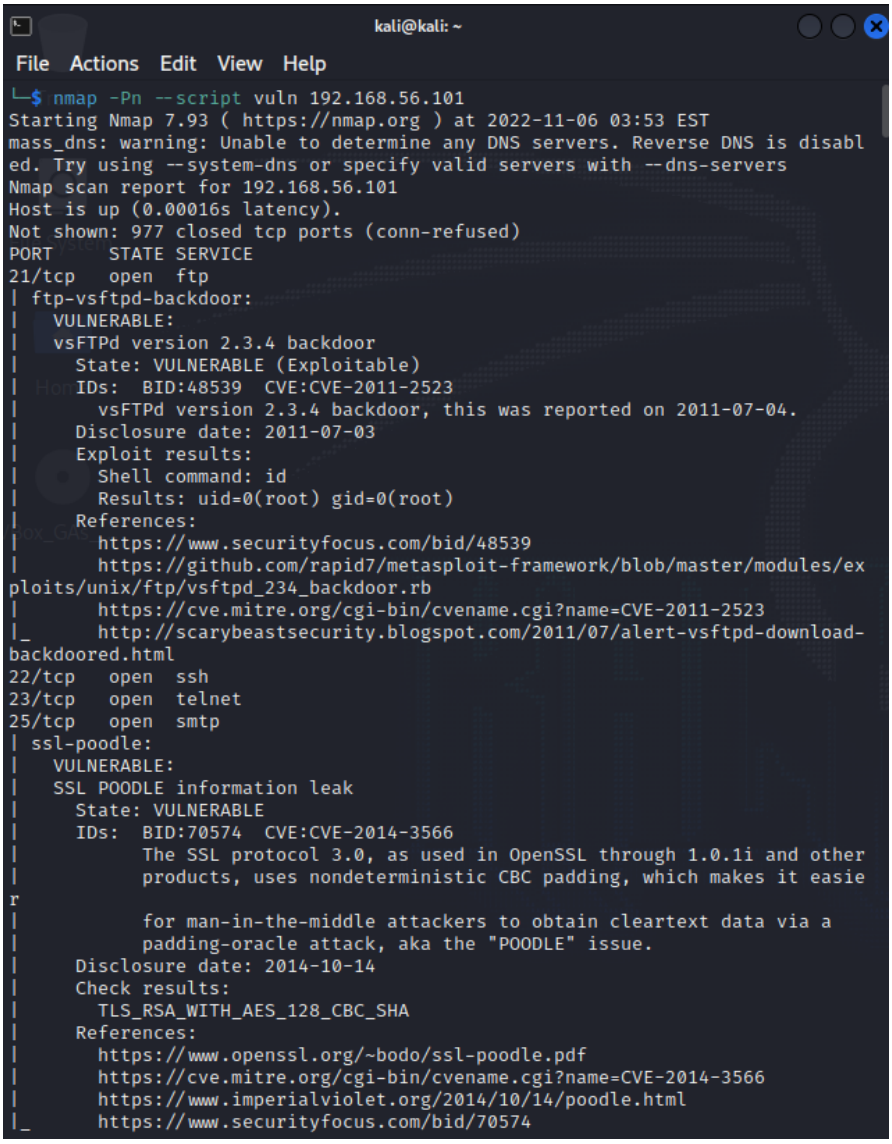
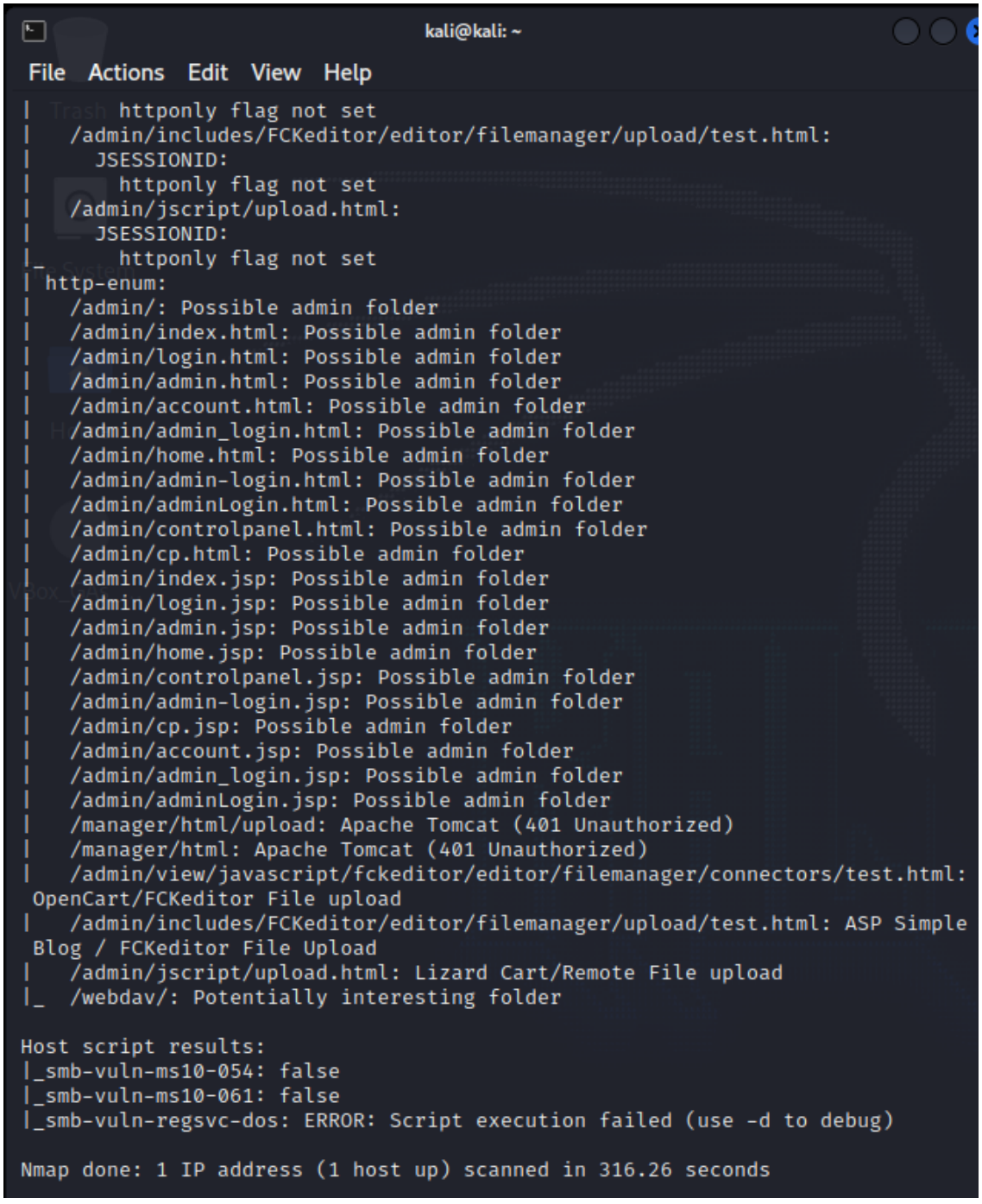


Figura 44

Ejecución herramienta NMAP al servidor vulnerable: Escáner completo de todos los puertos y redes (2/3).

Figura 45

Ejecución herramienta NMAP al servidor vulnerable: Escáner completo de todos los puertos y redes (3/3).



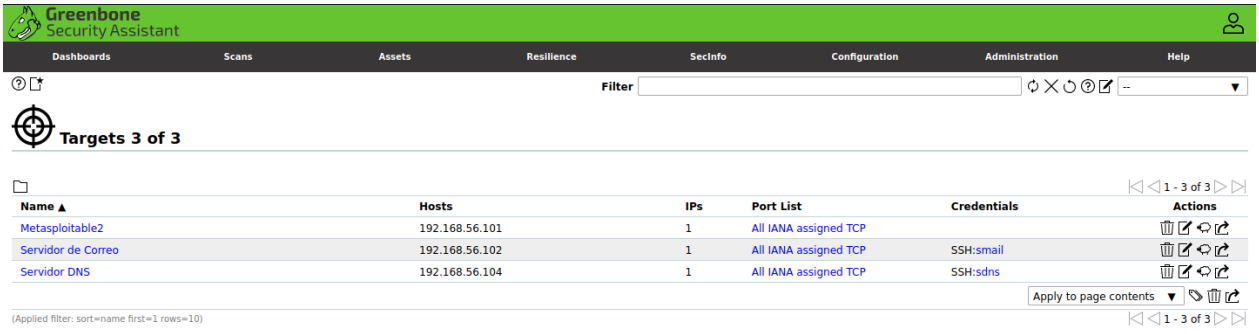
Al observar los resultados obtenidos tras la ejecución del script de análisis de vulnerabilidades se evidenció que fácilmente es posible explotar todas las vulnerabilidades que este presenta. En los detalles se evidencia que las configuraciones de archivos son débiles y los servicios de seguridad se encuentran deshabilitados. Existen puertas abiertas las cuales pueden ser accedidas por profesionales en ramas de ciberseguridad y extraer información sensible o de gran valor de la empresa. Este análisis al servidor vulnerable nos permitió evidenciar lo que puede presentarse y los riesgos que estas vulnerabilidades traen.

5.2.2. OpenVAS.

Como se mencionó previamente, esta herramienta analiza vulnerabilidades, razón por la cual para usar esta herramienta solo se requirió de la dirección IP del equipo y el nombre del dispositivo. Para ello nos dirigimos al apartado de configuración y seleccionamos “Targets” que son los dispositivos objetivos.

Figura 46

Dispositivos definidos en OpenVAS: Servidores objetivos.

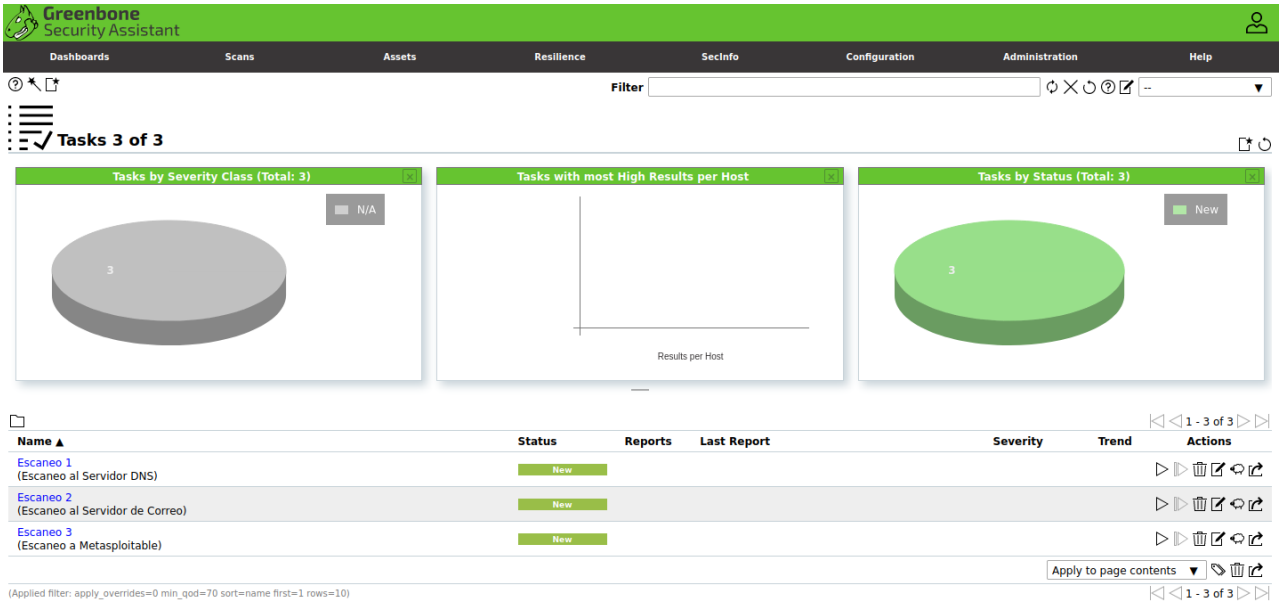


Una vez establecidos los objetivos para el análisis se procedió a realizar el escaneo de vulnerabilidades con las funcionalidades de la herramienta.

Es importante haber definido las tareas de análisis que se van a realizar.

Figura 47

Tareas definidas en OpenVAS para los servidores objetivos.



5.2.2.1. Servidor DNS y Servidor de Correo.

Servidor DNS

Se ejecutó la tarea asignada al objetivo correspondiente. A continuación, la tarea pasó por un proceso, empezando por la solicitud para hacer el descubrimiento de red y vulnerabilidades del equipo informático, como por ejemplo la identificación de los puertos abiertos y los servicios que en ellos se ejecutan, seguridad de los equipos, fallos en la seguridad, etc.

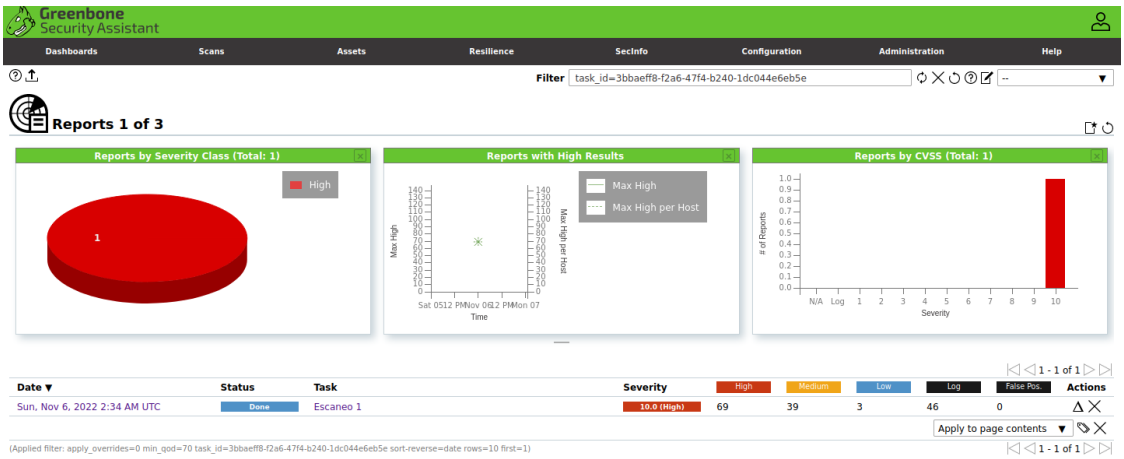
Figura 48

Petición de análisis hacia el Servidor DNS por parte de OpenVAS.

Cuando ha finalizado el análisis de vulnerabilidades del servidor DNS en este caso, se observa que el estado del análisis a llegado al 100% y se ha emitido un reporte.

Figura 49

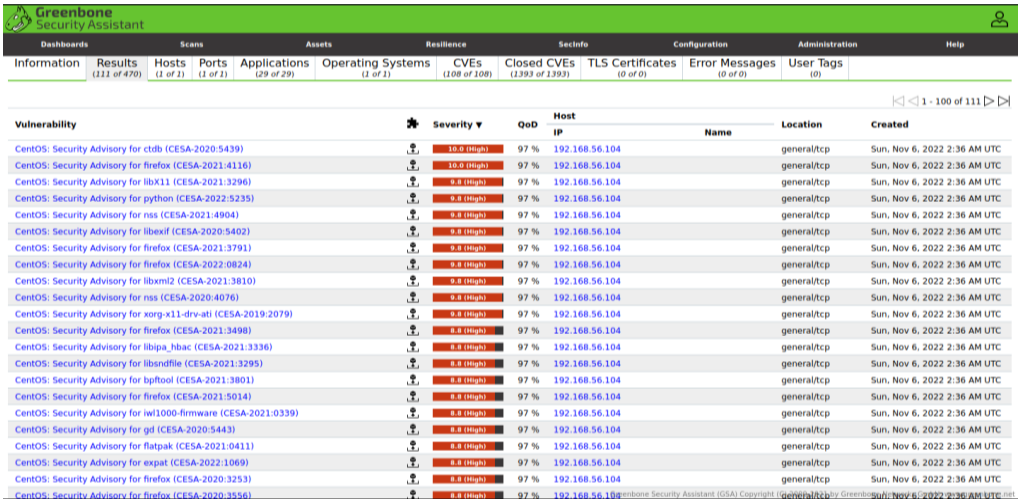
Ejecución de análisis de vulnerabilidades con OpenVAS al Servidor DNS.



Se analizó el reporte entregado por OpenVAS. En el apartado de resultados es la pestaña en la cual encontramos las fallas de seguridad y vuñnerabilidades presentes en el equipo del Servidor DNS. Es importante atender las vulnerabilidades que se presentaron de nivel alto ya que son las que presentan más riesgo para nuestro dispositivo.

Figura 50

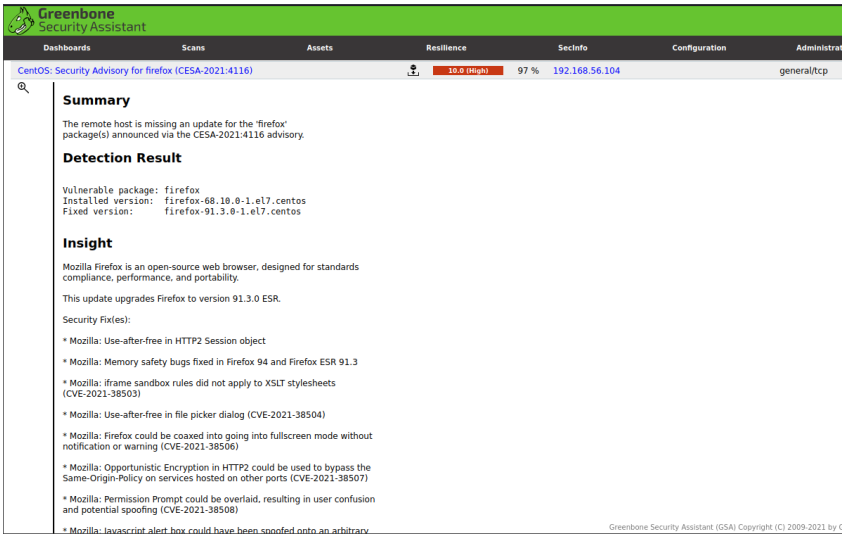
Vulnerabilidades halladas en el Servidor DNS.



Al entrar al detalle de una vulnerabilidad encontrada de nivel crítico, nos brindó una descripción de lo ocurrido y la razón de la vulnerabilidad como se puede observar en la imagen que se presenta a continuación.

Figura 51

Descripción de vulnerabilidad de alto nivel del Servidor DNS.



Revisando a detalle, la mayoría de las vulnerabilidades de nivel alto se debe a falta de actualizaciones en los paquetes de la aplicación o servicios. Como se observó, la falta de actualizaciones se presenta por parte de aplicaciones del servidor como es el caso de “Firefox”, aplicación que no se usa debido a que el servidor es usado para brindar un servicio en específico y no como un dispositivo de trabajo. Sin embargo, otros servicios que no cuentan con las ultimas actualizaciones son parte del sistema operativo, en este caso de CentOS 7 y estos servicios si deben ser actualizados, puesto que, esas vulnerabilidades si pueden ser explotadas.

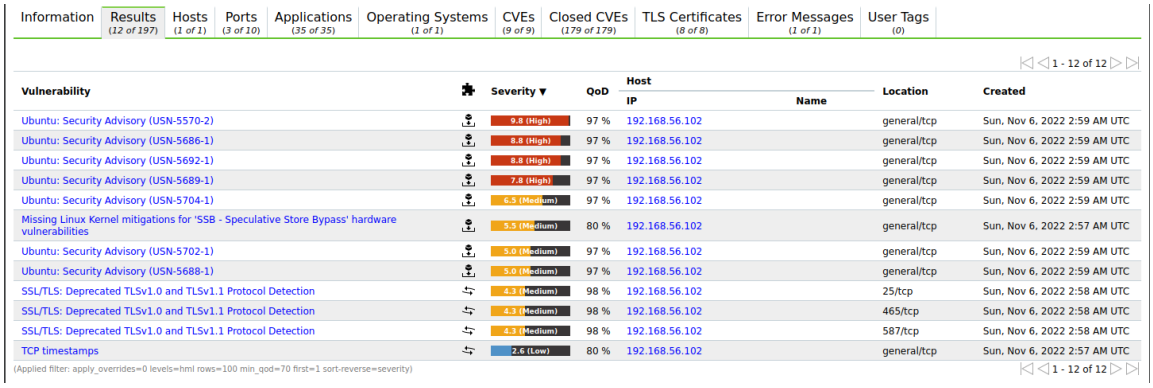
Al realizar el análisis de las vulnerabilidades de nivel medio pudimos encontrar la misma razón del por qué se presentan estas vulnerabilidades y se debe a la falta de actualizaciones. Al tomar una vulnerabilidad específica como es el caso del servicio “bind” el cual se requiere para la configuración del servidor DNS, se deben actualizar a los últimos parches para evitar posibles ataques debido a esta vulnerabilidad.

Servidor de Correo

Para el análisis del servidor de correo, se procedió del mismo modo del escaneo del servidor DNS, con la diferencia que se seleccionó la tarea correspondiente al Servidor de Correo.

Figura 52

Vulnerabilidades halladas en el Servidor de Correo.



Information | Results (12 of 197) | Hosts (1 of 1) | Ports (3 of 10) | Applications (35 of 35) | Operating Systems (1 of 1) | CVEs (9 of 9) | Closed CVEs (179 of 179) | TLS Certificates (8 of 8) | Error Messages (1 of 1) | User Tags (0)

1 - 12 of 12

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Ubuntu: Security Advisory (USN-5570-2)	9.8 (High)	97 %	192.168.56.102		general/tcp	Sun, Nov 6, 2022 2:59 AM UTC
Ubuntu: Security Advisory (USN-5686-1)	8.8 (High)	97 %	192.168.56.102		general/tcp	Sun, Nov 6, 2022 2:59 AM UTC
Ubuntu: Security Advisory (USN-5692-1)	8.8 (High)	97 %	192.168.56.102		general/tcp	Sun, Nov 6, 2022 2:59 AM UTC
Ubuntu: Security Advisory (USN-5689-1)	7.8 (High)	97 %	192.168.56.102		general/tcp	Sun, Nov 6, 2022 2:59 AM UTC
Ubuntu: Security Advisory (USN-5704-1)	6.5 (Medium)	97 %	192.168.56.102		general/tcp	Sun, Nov 6, 2022 2:59 AM UTC
Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware vulnerabilities	5.5 (Medium)	80 %	192.168.56.102		general/tcp	Sun, Nov 6, 2022 2:57 AM UTC
Ubuntu: Security Advisory (USN-5702-1)	5.0 (Medium)	97 %	192.168.56.102		general/tcp	Sun, Nov 6, 2022 2:59 AM UTC
Ubuntu: Security Advisory (USN-5688-1)	5.0 (Medium)	97 %	192.168.56.102		general/tcp	Sun, Nov 6, 2022 2:59 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.56.102		25/tcp	Sun, Nov 6, 2022 2:58 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.56.102		465/tcp	Sun, Nov 6, 2022 2:58 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.56.102		587/tcp	Sun, Nov 6, 2022 2:58 AM UTC
TCP timestamps	2.6 (Low)	80 %	192.168.56.102		general/tcp	Sun, Nov 6, 2022 2:57 AM UTC

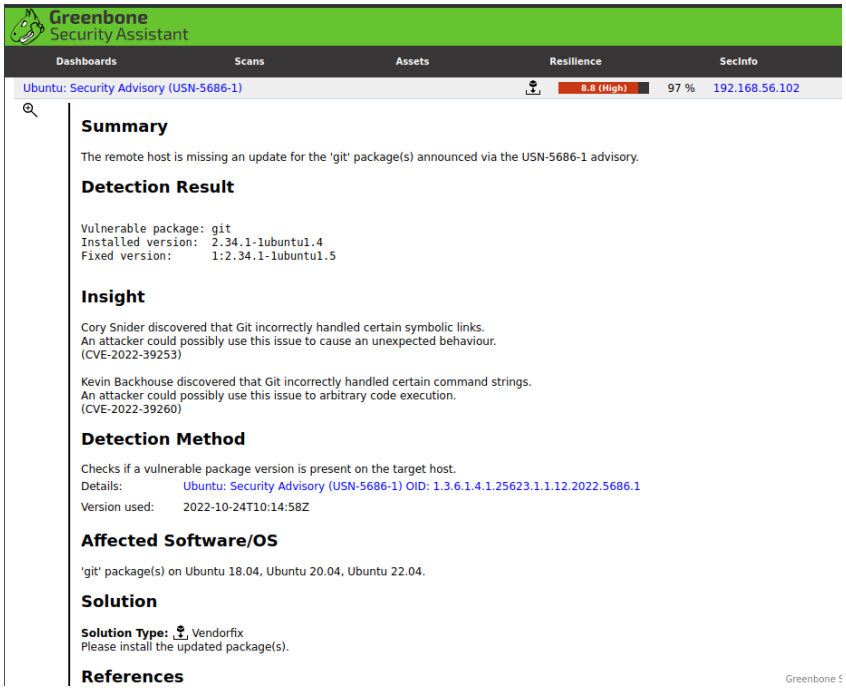
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 12 of 12

Al analizar los resultados del análisis de vulnerabilidades del Servidor de Correo pudimos observar que dado al sistema operativo que maneja este servidor (Ubuntu Server) posee menos vulnerabilidades de actualizaciones que el servidor de DNS analizado previamente. Del mismo modo las vulnerabilidades de alto nivel se deben a la falta de actualizaciones de paquetes. Podemos concluir que posiblemente existen menos vulnerabilidades de actualizaciones dado que el sistema operativo es diseñado para trabajar como servidor mismo.

Figura 53

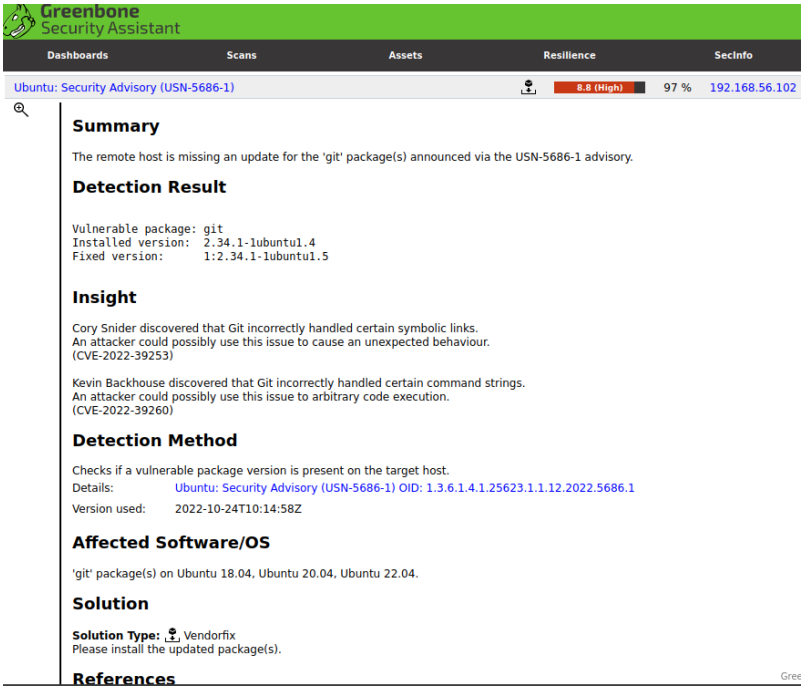
Descripción de vulnerabilidad de nivel alto en el Servidor de Correo.



Revisadas las vulnerabilidades de nivel medio, encontramos una vulnerabilidad que hace referencia al hardware, por lo que se recomienda actualizar el Kernel de Linux para mitigar la posible vulnerabilidad de SSB.

Figura 54

Descripción de otra vulnerabilidad de nivel alto en el Servidor de Correo.

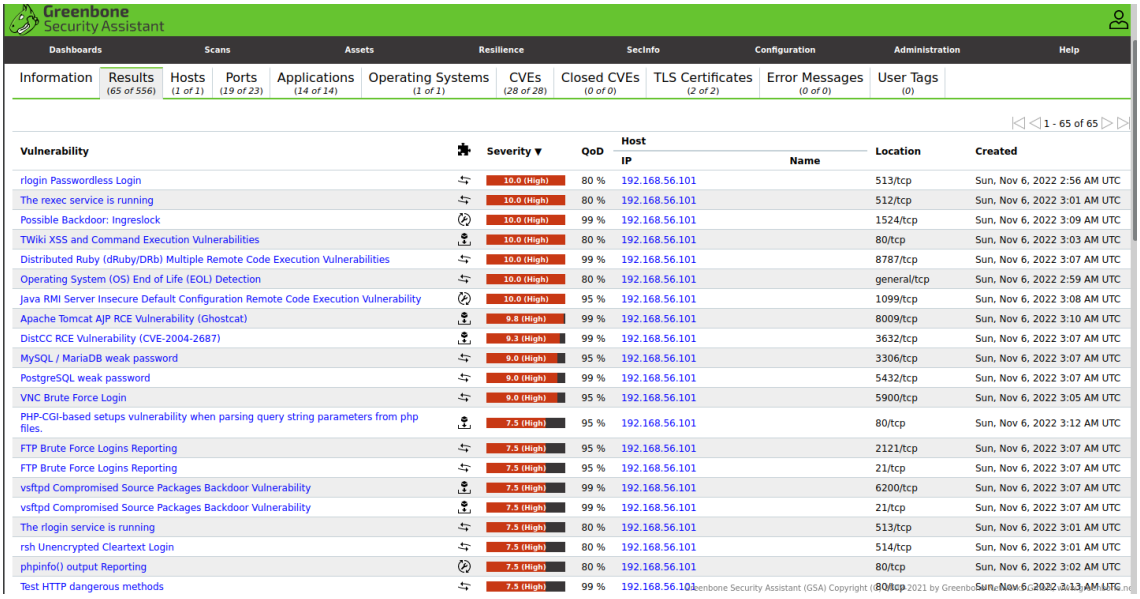


5.2.2.2. Servidor Metasploitable2.

Al igual que los servidores previamente analizados se seleccionó la tarea correspondiente para este análisis y al finalizar se obtuvieron los siguientes resultados.

Figura 55

Vulnerabilidades de alto nivel halladas en el Servidor Vulnerable.



Con OpenVAS el tiempo de escaneo es mucho más largo ya que se ejecutan miles de funciones simultáneamente para encontrar la mayor cantidad de fallos de configuración y vulnerabilidades posibles.

Como su pudo observar en las Figuras anteriores, las vulnerabilidades que se presentan aquí ya no fueron de actualizaciones de paquetes del sistema operativo o de algunas aplicaciones o servicios, aquí ya se observaron vulnerabilidades en la configuración de servicios, así como autentificaciones débiles (contraseñas comunes).

Si nos enfocamos en las bases de datos se pudo observar que el servidor vulnerable contiene fallas en archivos script, así como en la configuración de los mismos, volviéndolos vulnerables.

Figura 56

Vulnerabilidades de medio nivel halladas en el Servidor Vulnerable.

Al analizar las vulnerabilidades halladas de nivel medio, se observó posee certificados SSL caducados, así como protocolos de comunicaciones que no se encuentran encriptados, lo que puede dar paso a explotar dicha vulnerabilidad como un atacante.

Comparando los servidores empresariales implementados (Servidor DNS y Servidor de Correo) con el servidor vulnerable (Metasploitable2) pudimos concluir que son servidores robustos en cuanto a seguridad puesto que las únicas vulnerabilidades que se encontraron en ambos servidores configurados fueron falta de parches o actualizaciones de ciertos servicios, por lo que la solución óptima corresponde a realizar un chequeo constante de las versiones tanto de servicios y aplicaciones como del sistema operativo, para disminuir el riesgo de un posible ataque.

Adicionalmente se concluyó que esta herramienta proporciona gran cantidad de información sobre las vulnerabilidades encontradas puesto que genera un reporte muy completo, además, es posible mantener en constante monitoreo nuestros equipos informáticos ya que permite programar los análisis y guarda los reportes en su repositorio para que el administrador de TI pueda evaluar los resultados y proponer soluciones.

5.2.3. OWASP-ZAP.

Esta herramienta tiene varias funcionalidades como realizar ataques de inyección SQL, detección de errores en los archivos XML, análisis de vulnerabilidades de equipos informáticos, entre otras funciones.

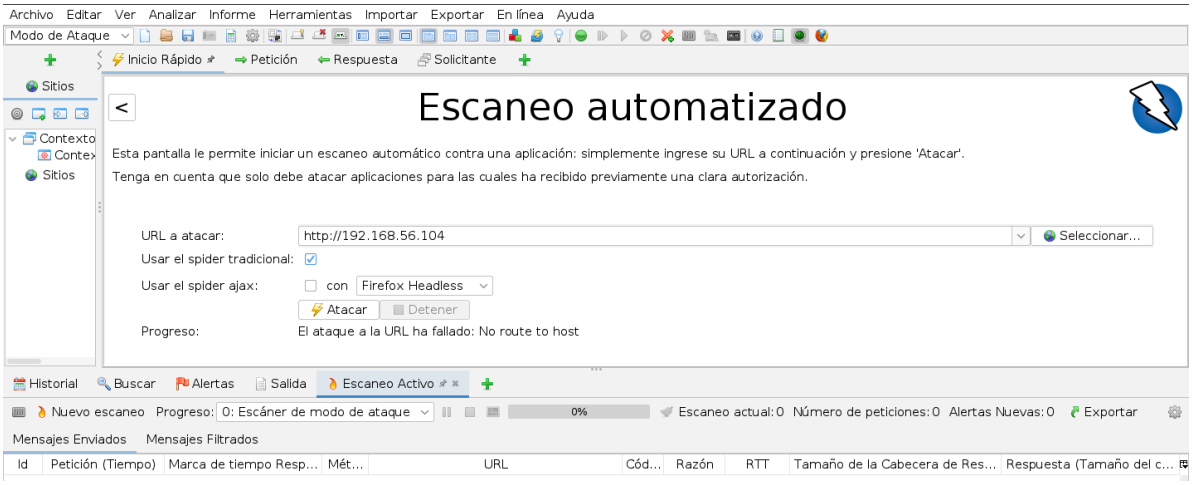
5.2.3.1. Servidor DNS y Servidor de Correo.

Servidor DNS

La herramienta OWASP-ZAP fue diseñada para analizar y encontrar vulnerabilidades de sitios web que se encuentren alojados en nuestros servidores, razón por la cual podemos observar que para nuestro servidor no se han encontrado resultados. En el servidor DNS no se encuentra levantado ninguna página web, únicamente se encuentra configurado para proporcionar los nombres de dominio al resto de servidores.

Figura 57

Resultados de OWASP-ZAP para el Servidor DNS.

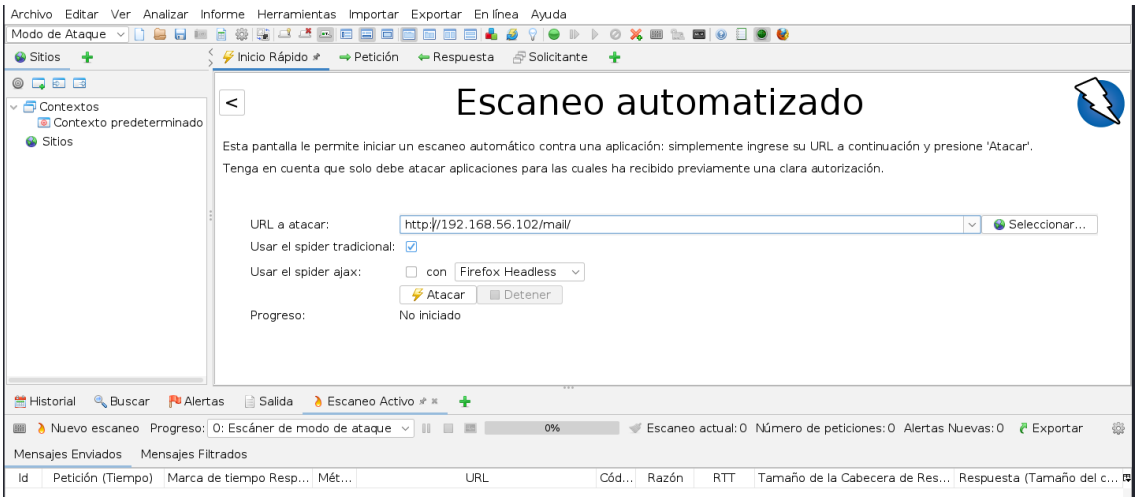


Servidor de Correo

Se seleccionó la dirección a la cual está asociada el servidor de correo electrónico el cual pertenecería a la empresa, para realizar el ataque.

Figura 58

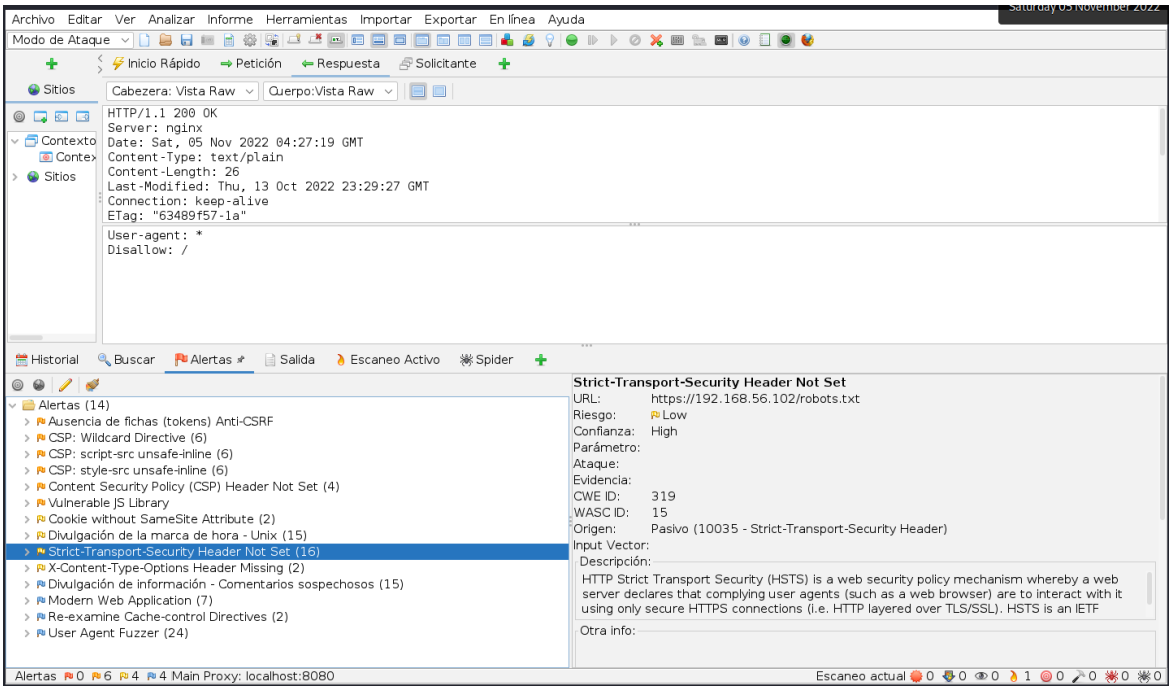
Escaneo automatizado OWASP-ZAP para Servidor de Correo.



Se puede observar ya realizado el análisis que, al ser un ataque directamente a un sitio web (sitio web levantado por el servidor para correo electrónico empresarial) existen varias alertas de las cuales podrían existir vulnerabilidades y ser explotadas en caso de ser graves, razón por la cual se deben analizar cada una de las alertas y comprobar que no sean fallos en el diseño de la web (comúnmente encontrados).

Figura 59

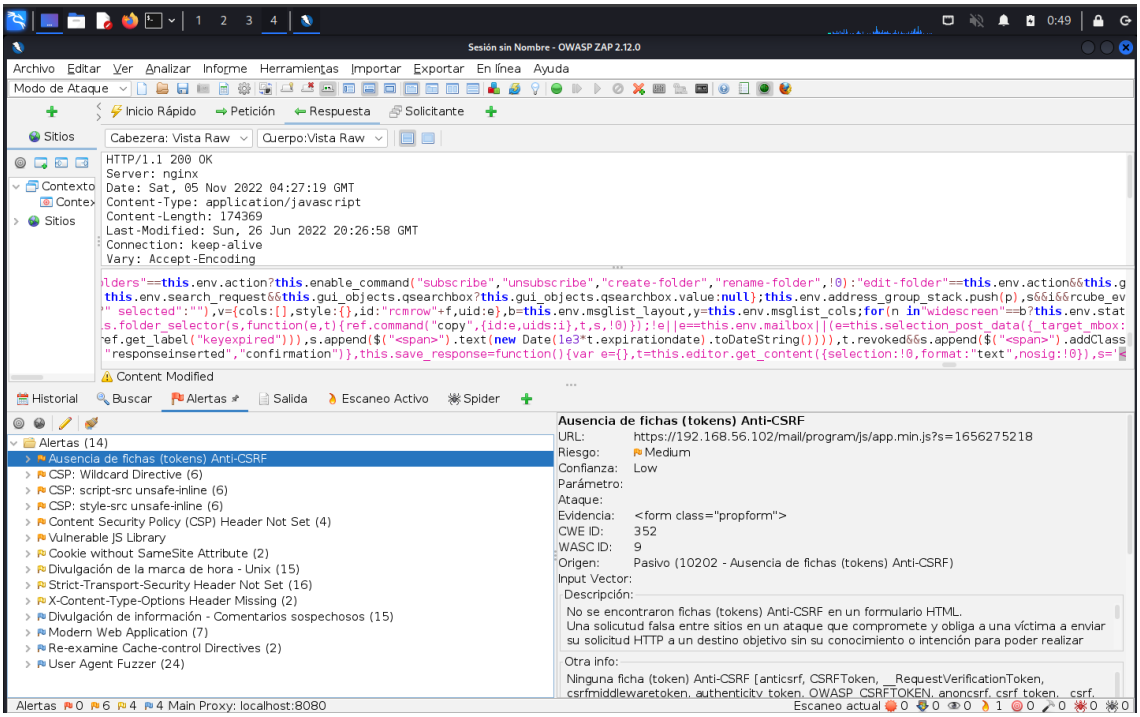
Vulnerabilidades encontradas en Servidor de Correo.



Tomando como ejemplo la Figura 59, se presentó la existencia de una vulnerabilidad al no existir tokens que garanticen las peticiones hacia el sitio web original, razón por la cual es posible que se pueda realizar un ataque, ya que, un usuario (víctima) puede hacer peticiones sin saberlo a un sitio web objetivo (atacante); esta vulnerabilidad explota la confianza que un sitio web le proporciona a un usuario.

Figura 60

Detalle de vulnerabilidad en Servidor de Correo.



Analizando la vulnerabilidad se pudo proponer una posible solución, que consiste en mejorar el diseño y la arquitectura de la página web incluyendo librerías que usen un token para asegurar la secuencia entre sitios web. También se tomó en consideración que el servidor de correo electrónico fue previamente desarrollado por la comunidad, lo que no garantiza una fácil edición en el diseño de la página web en cuestión; lo que da paso a otra solución, contratación de servicio de correo electrónico, donde al usar esta aplicación sea posible hablar con el encargado del software y pueda realizar las modificaciones correspondientes para reducir las vulnerabilidades que se puedan encontrar.

Es importante tener en consideración que todas las alertas que presenta la herramienta no siempre son vulnerabilidades, es importante leer la descripción y entender a que ha hecho

referencia la alerta para identificar si puede representar o no una vulnerabilidad. Por ejemplo, en la alerta de “Content Security Policy” ha presentado como descripción que se debe mantener autenticación en el sitio web, por lo cual no hemos clasificado como vulnerabilidad ya que entendemos que al ser un sitio web de correo electrónico, un usuario siempre posee credenciales para su uso. De igual manera, otra de las alertas halladas fue la falta de seguridad para acceder al sitio web de manera externa, sin embargo, se entiende que el ataque está realizado desde la red interna de la empresa por lo cual la solución propuesta (y también definida por OWASP-ZAP) es la configuración de políticas de seguridad de acceso en los equipos de seguridad de la red como son los Firewall, por ejemplo.

5.2.3.2. Servidor Metasploitable2.

Al haber analizado nuestro servidor vulnerable, podemos encontrar varias alertas a diferencia de nuestro servidor DNS ya que como se mencionó en capítulos anteriores, este fue diseñado para verificar la mayor cantidad de vulnerabilidades posibles, además este servidor si cuenta con servicios de página web para poder analizarlo con esta herramienta.

Figura 61

Análisis del Servidor vulnerable con OWASP-ZAP

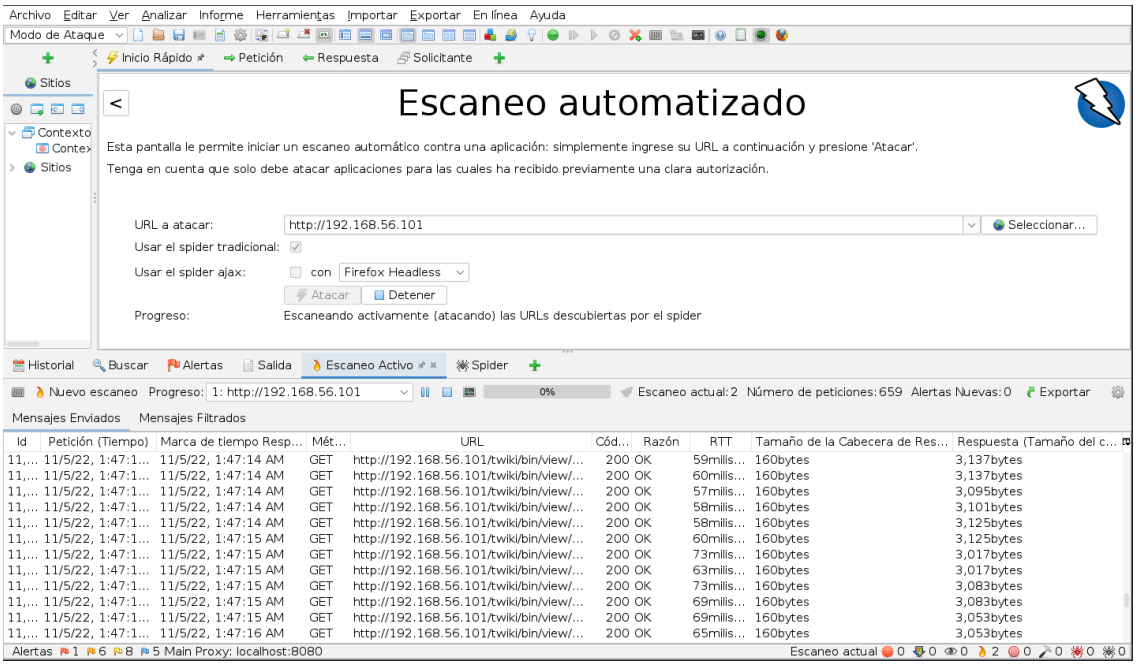
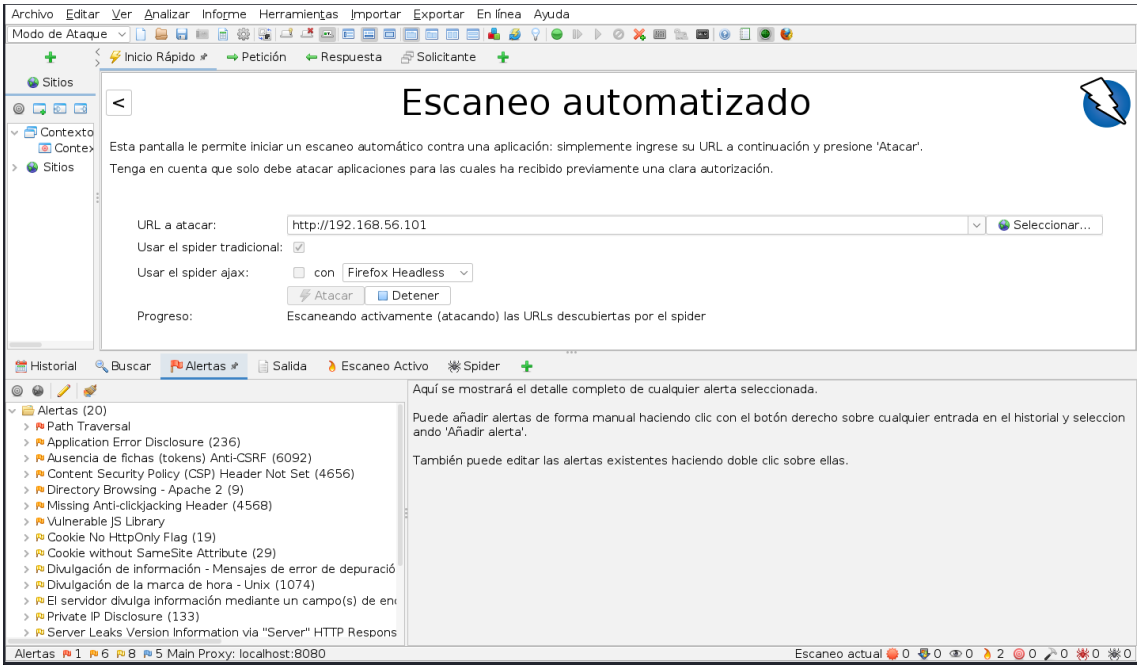


Figura 62

Resultados análisis Servidor vulnerable.



Sería muy complicado analizar todas las vulnerabilidades encontradas por OWASP-ZAP ya que es un servidor que se encuentra completamente vulnerable, no obstante, si es importante revisar todas las alertas para entender la razón por las cuales se presentaron, así como aclarar el panorama en caso de presentarse dichas vulnerabilidades ya en nuestros servidores reales.

CAPÍTULO VI: ELABORACIÓN DE METODOLOGÍA DE ANÁLISIS CON BASE EN LOS RESULTADOS OBTENIDOS

6. Metodología para análisis de vulnerabilidades de servidores de una red empresarial

6.1. Precondiciones antes de aplicar la metodología.

Antes de la ejecución de la metodología para el análisis de vulnerabilidades se debieron tomar en consideración ciertas precondiciones las cuales son detalladas a continuación.

Es importante haber realizado una evaluación de que tipo de vulnerabilidades se requiere analizar:

- Hardware o
- Software.

Ya habiendo seleccionado el tipo de análisis de vulnerabilidades que se requiere evaluar, se procede a realizar la búsqueda de varias herramientas que permitan cumplir tanto con los objetivos de la búsqueda como con la calidad de los resultados obtenidos.

6.1.1. Seleccionando segmentos o dispositivos a ser analizados.

El análisis de vulnerabilidades puede realizarse de forma general a la red empresarial, incluyendo todos los dispositivos que se encuentran en esta, como, por ejemplo: Firewall, Routers, Switches, ordenadores, servidores, etc. No obstante, también es posible realizar análisis a ciertos segmentos de la red, como, por ejemplo: dispositivos de la red (Routers y Switches) o equipos informáticos (ordenadores y servidores); o de forma más específica a un solo equipo o dispositivo que se encuentre dentro de la red empresarial.

La selección del análisis dependerá del enfoque sé que le quiera dar y dependiendo de esta selección, dependerá también las herramientas para dicho análisis.

6.1.2. Seleccionando las herramientas para análisis.

Las herramientas para el análisis respectivo deben estar en la capacidad de abarcar la mayor cantidad de funciones para un análisis a profundidad. Es imprescindible haber testeado varias herramientas, puesto que, al probar varias herramientas es posible realizar una selección más objetiva basada en la información de los resultados arrojados, además, así se pueden descartar herramientas que cumplen con su propósito pero proporcionan falsos positivos, es decir, arrojan vulnerabilidades que probablemente no representen amenazas, sino que únicamente se evalúan, por ejemplo, puertos abiertos, pero, no se toma en consideración la configuración o protocolos de seguridad que se encuentren implementados para el servicio al cual se encuentra asociado dicho puerto.

Se considera una buena práctica seleccionar algunas herramientas que ejecuten funciones similares, puesto que, de este modo es posible contrastar la información que arroja una herramienta con la información de proporcionada por la otra.

6.1.3. Generalidades para emplear una metodología.

Una vez seleccionadas las herramientas que cumplan con los objetivos para el escaneo, es posible mencionar que para analizar vulnerabilidades ya sean de hardware o software, se puede seguir lo mencionado en “Seleccionando segmentos o dispositivos a ser analizados” así como en “Seleccionando las herramientas para análisis”, pues, de forma general la información que ahí se describe, ha sido detallada desde un enfoque aplicable a cualquier análisis.

6.2. Proceso metodológico para análisis de vulnerabilidades de servidores de una red.

El proceso que se detalló a continuación fue realizado en base a los resultados obtenidos en el capítulo anterior, siguiendo las buenas prácticas de calidad para escaneo de vulnerabilidades.

6.2.1. Evaluación del estado de los servidores a analizarse.

La revisión de la configuración de los servicios que se encuentran ejecutando en nuestros servidores es primordial para entender la situación en la que están los servidores; la revisión de la documentación y de las versiones aplicadas ayudan a entender de mejor manera las vulnerabilidades que han sido parchadas.

La revisión de registros de monitoreos realizados previamente es considerada de gran ayuda antes de realizar cualquier proceso de análisis ya que nos ayuda a entender los problemas que se han presentado en el pasado y con ello saber manejar y corregirlos rápidamente en caso de volverse a presentar.

6.2.2. Escaneo de vulnerabilidades con herramientas de Software Libre.

Las herramientas presentadas para realizar este tipo de análisis en específico han sido seleccionadas por la calidad de los resultados obtenidos. Con estas herramientas es posible obtener reportes claros de los análisis realizados, los cuales son de vital importancia para poder entender la razón de las vulnerabilidades que se han presentado.

En esta fase es muy importante definir las tareas y las funcionalidades a emplearse de cada tarea dependiendo del tipo de análisis que se desee realizar. Se hace énfasis en las herramientas presentadas para realizar un buen análisis como NMAP y OpenVAS comparten algunas de sus funcionalidades, lo que nos ayuda a contrastar que la información proporcionada por una herramienta tenga relación con los resultados de la otra herramienta en cuestión.

Se tomó como consideración que pueden existir otro tipo de servidores dentro de una red empresarial como es el caso de servidores web, por lo cual emplear un análisis con la herramienta OWASP-ZAP permitirá abarcar una mayor cantidad de vulnerabilidades que puedan presentarse.

La documentación disponible por cada herramienta permite explotar el potencial de cada herramienta por lo cual, una buena práctica del uso de estas herramientas consiste en analizar todas las funcionalidades presentes en cada herramienta para poder realizar un análisis exitoso sin dejar de lado ninguna posible vulnerabilidad sin ser analizada.

6.2.3. Análisis de reportes proporcionados por las herramientas.

No es suficiente la ejecución del escaneo de vulnerabilidades para los sistemas informáticos, se requiere de una comprensión de los reportes entregados luego del análisis ejecutado ¿Por qué? Pues no nos sirve de nada que las herramientas entreguen información de las vulnerabilidades encontradas en los servidores, si no podemos comprender la razón por la que se presentan y mucho menos poder plantear soluciones si no conocemos las causas para presentarse dicha vulnerabilidad.

Otro factor determinante por lo cual es indispensable el análisis de los resultados obtenidos en los reportes, es que posiblemente, pueda presentarse una supuesta vulnerabilidad en nuestro sistema, sin embargo, al no analizar la fuente de la "vulnerabilidad" desconozcamos que el supuesto fallo en verdad es primordial para la prestación de algún servicio. Poniendo como ejemplo se puede hablar de la siguiente manera: El puerto "ab" se encuentra abierto y ejecuta un servicio XY configurado por parte de la empresa. Dicho servicio pertenece a una aplicación diseñada por parte de la misma empresa y es fundamental para el funcionamiento de esta; al analizar los puertos por diversas herramientas se evidenciará que el puerto es considerado como puerta trasera ya que se está ejecutando un servicio de tipo "desconocido". Si nosotros no analizamos los resultados de los reportes probablemente se proponga una solución errónea como

cerrar el puerto, lo que afectaría gravemente al funcionamiento de la aplicación y por ende a la empresa misma.

6.2.4. Contraste de información obtenida de las herramientas empleadas.

Como se mencionó en fases anteriores, las herramientas integran algunas funcionalidades similares a las de otra herramienta, por lo cual, contrastar información de los resultados obtenidos por una herramienta con los proporcionadas por otra, permite que exista coherencia en los resultados para poder generar un informe final donde se integren los resultados de todas las herramientas utilizadas.

La importancia de verificar los resultados obtenidos de diferentes fuentes permite identificar si la información entregada por parte de la aplicación no corresponde a falsos positivos de vulnerabilidades, es decir, identificación de supuestas vulnerabilidades, pero, que no pueden ser catalogadas como tal.

6.2.5. Elaboración del reporte final de los resultados obtenidos.

En esta fase se realiza un consolidado de todos los análisis realizados en conjunto con el contraste de información de las herramientas empleadas. El reporte que se debe generar debe ser detallado con la descripción de la vulnerabilidad, así como la causa por la que se ha presentado la vulnerabilidad; de ser posible el reporte debe contener el origen de la vulnerabilidad y como se la encontró, toda esta información se la puede encontrar en los reportes emitidos por cada herramienta.

Es muy importante esta fase, pues de esta fase depende la propuesta de soluciones para las vulnerabilidades que han sido encontradas luego del análisis. Además, el reporte que se generará será de utilidad para el próximo análisis que se vaya a ejecutar, puesto que, permite evaluar la

situación en la que se encontraba la empresa y si las vulnerabilidades halladas han sido solucionadas.

6.2.6. Propuesta de soluciones o mejoras ante los resultados obtenidos.

Se puede considerar como la última fase del proceso antes de repetirlo periódicamente (monitoreo y mejora continua). La propuesta soluciones con base los resultados obtenidos en el reporte generado, significa una reducción de probabilidad de que un atacante pueda explotar una vulnerabilidad convirtiéndola en una amenaza para la empresa.

Las mejoras recurrentes en la seguridad de los equipos informáticos permiten mantener un sistema robusto reduciendo la probabilidad de presentar vulnerabilidades en la configuración de servicios.

Mantener actualizados a las últimas versiones los servicios, sistema operativo o complementos de aplicaciones brindarán más seguridad a los equipos, pues las actualizaciones implementan parches en la seguridad y evitan vulnerabilidades que se han encontrado en versiones pasadas.

CAPÍTULO VII: CONCLUSIONES Y RECOMENDACIONES

7. Conclusiones y Recomendaciones

7.1. Conclusiones

- Los términos vulnerabilidad y amenaza están relacionados más no se deben confundir como sinónimos; una vulnerabilidad es una debilidad o fallo en la configuración de algún sistema informático poniendo en riesgo la seguridad de este, pues un atacante puede aprovechar esta debilidad, a esto se le conoce como amenaza, es decir, el aprovechamiento o explotación de una vulnerabilidad con un fin específico como comprometer: la información alojada en el sistema vulnerable o la seguridad del mismo sistema.
- El análisis de vulnerabilidades es una de las etapas más cruciales para las pruebas de penetración, es semejante a la recopilación de información, no obstante, se tiene como objetivo específico la identificación de debilidades que puedan ser explotadas por un atacante. Dicha etapa es valiosa ya que la vulnerabilidad hace que el sistema quede expuesto a ataques cibernéticos.
- La utilización de un procedimiento o de una metodología para el análisis de vulnerabilidades permite realizar un análisis exitoso sin redundancia o brechas en la información encontrada, además da paso de una entrega de un informe de calidad que se encuentre completo y detallado con base en resultados coherentes del análisis realizado.
- Las vulnerabilidades encontradas hacen referencia a varios puertos abiertos, sin embargo, se evidenció mediante un análisis que dichos puertos pertenecen a los

servicios requeridos para la ejecución de tareas de los equipos informáticos y no de servicios maliciosos o puertas traseras abiertas como se evidenció los resultados del análisis del servidor vulnerable.

- Es importante tener claro que dichos ataques o escaneos se deben realizar bajo una aprobación del departamento de TI, ya que al ser ataques de penetración y forzosos, es posible meterse en problemas legales si se llega a descubrir que han sido realizados sin autorización.
- Los servidores con mayor cantidad de vulnerabilidades son aquellos que prestan algún tipo de servicios hacia los usuarios como el caso del servidor de correo electrónico puesto que este tipo de servidores alojan aplicaciones que generalmente son desarrolladas por terceros por lo que son más propensos a ser atacados; en caso de alojar aplicaciones desarrolladas por parte de la empresa, se deben tomar en consideración los aspectos de seguridad, ya que si existen vulnerabilidades dentro de la aplicación podría poner en riesgo el servidor encargado de proporcionar este servicio.
- Se puede considerar esta metodología como parte de una auditoría informática la cual realiza un análisis de vulnerabilidades de los sistemas de información, verificando la configuración de estos, ya que proporciona al auditor una guía referencial para realizar el procedimiento de auditar el área de sistemas informáticos, en otras palabras, el análisis de vulnerabilidades debe ser usado con fines para la mejora de la seguridad de los equipos informáticos.

7.2. Recomendaciones

- Analizar las vulnerabilidades de los equipos de una red determinada, permite conocer los posibles puntos débiles de la seguridad de los equipos informáticos de una red determinada por lo cual se recomienda realizarlo periódicamente y mantener actualizadas las herramientas de análisis con el fin de contar con repositorio actualizado de las vulnerabilidades halladas y de este modo poder mejorar la seguridad para poder tener sistemas más robustos.
- Para el análisis se utilizó una máquina virtual con un sistema operativo diseñado para ataques y pruebas de seguridad, razón por la cual se recomienda ejecutar el comando de actualización del sistema antes de ejecutar o utilizar alguna herramienta de Software en el servidor de Kali Linux, puesto que con ello nos aseguraremos de contar con todas las características y mejoras del sistema para un análisis exitoso.
- Si bien las herramientas de análisis de vulnerabilidades son de gran ayuda para encontrar debilidades o fallos en la configuración o en la seguridad de los sistemas, se recomienda contratar a un experto (Hacker Ético) quien se encarga de encontrar vulnerabilidades de una forma más fina por todo el conocimiento y preparación que ha adquirido, así como de lectura adecuada de reportes entregados por las herramientas y de este modo brindar mejores soluciones y óptimas.
- Contar con varias herramientas para el análisis de vulnerabilidades permite tener resultados más acertados por lo que se recomienda realizar un buen análisis al momento de seleccionar las herramientas para el escaneo, pues de estas depende la calidad de los resultados esperados.

- En los resultados obtenidos se observó que el puerto 22 perteneciente al servicio de conexión remota SSH, se encuentra abierto, por lo cual, se recomienda por seguridad que se deniegue el acceso a root por conexión SSH o deshabilitar el servicio SSH de no ser requerido.

BIBLIOGRAFÍA

DOÑA, Jesús; GARCÍA, Juan; LÓPEZ, Jesús; PASCUAL, Francisco & PASCUAL, Rubén. *Virtualización de Servidores. Una solución de Futuro, Área de Tecnología y Sistemas de Información*, [En línea] (Paper) Campus Universitario de Teatinos, Málaga - España. 2010. pp. 1-5. [Consulta: 2019-03-11]. Disponible en: http://www.redtauros.com/Clases/Gestion_SO/Sistemas_paravirtuales.pdf

Arias Paredes, Á. S. (2019). *Análisis de vulnerabilidades de servidores virtuales, caso práctico servicios web informativos de la ESPOCH* [Escuela Superior Politécnica de Chimborazo]. http://dspace.espoch.edu.ec/bitstream/123456789/13631/1/98T00269.pdf

Garzón, D. S., Carlos, J., Gomes, R., Vergara Torres, A., María, I., & Serrano, I. (n.d.). *Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala*. Edu.Co. Recuperado el 25 de agosto de 2022, de https://repository.javeriana.edu.co/bitstream/handle/10554/7467/tesis181.pdf?sequence=1&isAllowed=y

Márquez, A. (2011). *Virtualización de Servidores*. Universitat Politècnica de Catalunya.

Laura, C. (s/f). *Seguridad informática y seguridad de la información*. Universidad Piloto de Colombia.

Vega Briceño, E. (2021*). Seguridad de la información*. Editorial Científica 3Ciencias.

Molina, Y., & Luis, G. (s/f). Vulnerabilidades de los Sistemas de Información: una revisión Information System Vulnerabilities: A review. Edu.co. Recuperado el 26 de agosto de 2022, de https://dspace.tdea.edu.co/bitstream/handle/tdea/1398/Informe%20Vulnerabilidad%20sistemas.pdf?sequence=1&isAllowed=y

Arévalo-Cordovilla, & Ordoñez-Sigcho. (2020). Ciencias de la computación Artículo de investigación. 6, 835–846.

ISO/IEC 27000. (2016). Information technology–Security techniques–Information security management systems–Overview and vocabulary. https://www.iso.org/standard/66435.html

Engard, N. C. (2010). What is open source? En *Practical Open Source Software for Libraries* (pp. 3–11). Elsevier.

Gnuien?, ¿quién E. S. (s/f). *¿Qué es el Software Libre? - Proyecto GNU - Free Software Foundation*. Gnu.org. Recuperado el 8 de noviembre de 2022, de https://www.gnu.org/philosophy/free-sw.es.html

Qué es la virtualización: definición. (s/f). Microsoft.com. Recuperado el 8 de noviembre de 2022, de https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-virtualization/

¿Qué es un hipervisor? (s/f). Redhat.com. Recuperado el 8 de noviembre de 2022, de https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor

¿Qué es un hipervisor? (2022, octubre 19). VMware. https://www.vmware.com/latam/topics/glossary/content/hypervisor.html

Simic, S. (2021, febrero 9). *Virtualbox vs VMware: Detailed comparison {how to choose?}*. Knowledge Base by PhoenixNAP; phoenixNAP. https://phoenixnap.com/kb/virtualbox-vs-vmware

Virtualization technology & virtual machine software: What is virtualization? (2022, agosto 11). VMware. https://www.vmware.com/latam/solutions/virtualization.html

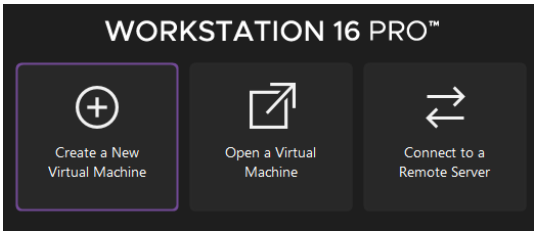
GLOSARIO DE TÉRMINOS

- **Host:** Se define un host a una computadora que es capaz de brindar servicios como almacenamiento y procesamiento de datos, envío de correos electrónicos, acceso a internet, entre otros.
- **GNU:** Sistema Operativo basado en Unix, diseñado para el diseño y desarrollo de software libre.
- **CPU:** La unidad central de procesamiento es quien se encarga del cálculo y cómputo de todas las instrucciones pedidas por todos los softwares presentes en la computadora.
- **Kernel:** Es definido como el núcleo o corazón del sistema operativo, el cual permite compatibilidad y comunicación entre software y hardware.
- **Contenedores:** es un tipo de virtualización donde únicamente se virtualiza de forma aislada la aplicación que se virtualiza en conjunto con sus servicios.
- **Vulnerabilidad de día 0 (Vulnerability 0 days):** Es una vulnerabilidad que no se ha presentado con anterioridad en ningún sistema, es decir, no existe registro de haberse presentado en algún sistema informático a nivel mundial, razón por la cual se complica su detección y mitigación.
- **Benchmark**: es una prueba que sigue una línea base para la medición del rendimiento ya sea de una aplicación, hardware o de un sistema.

ANEXOS

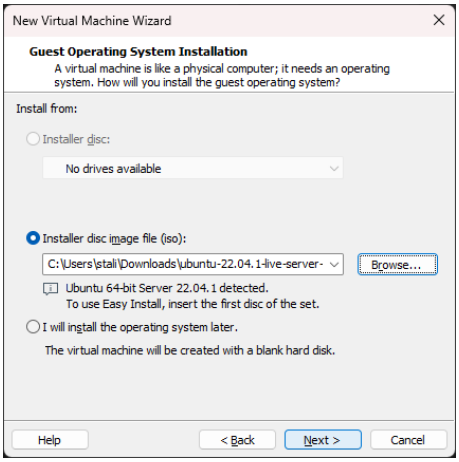
Anexo A: Creación de máquinas virtuales.

En VMware WorkStation 16 seleccionamos la opcion de crear una nueva máquina virtual.

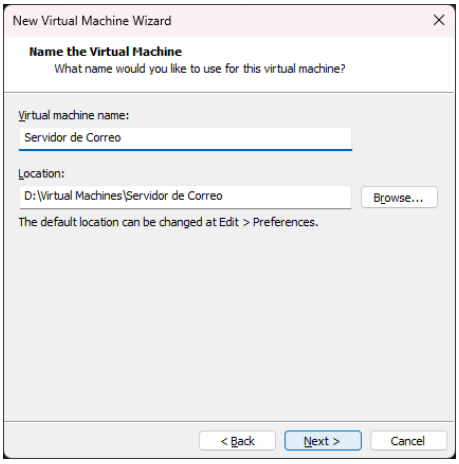


Selecionamos la opcion por defecto ya que no requerimos la creacion de una máquina virtual con características más especializadas.

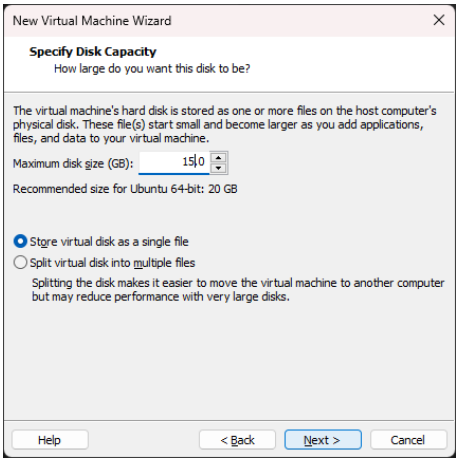
Procedemos a seleccionar nuestro archivo *.iso* de nuestro sistema operativo; una vez seleccionado, VMware detectará de qué sistema operativo se trata.



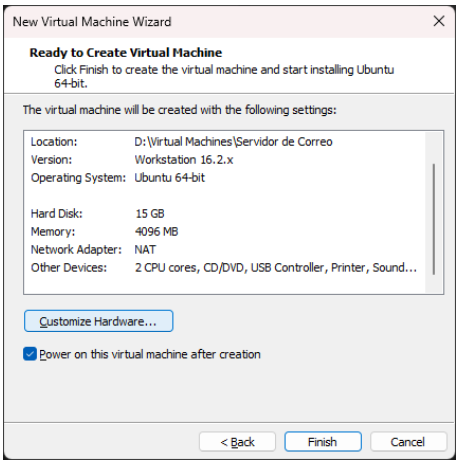
Procedemos a dar un nombre a nuestra máquina virtual y del mismo modo seleccionamos la ubicación donde se almacenarán dichos archivos.



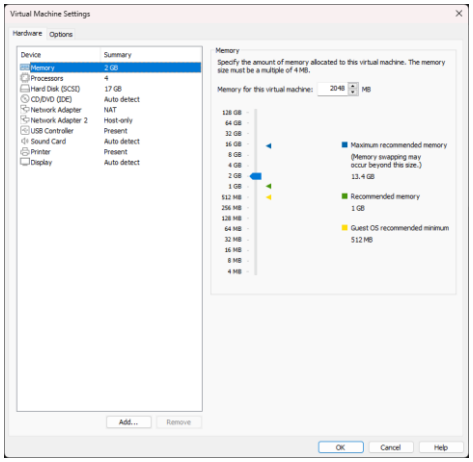
Asignamos la capacidad de almacenamiento a nuestra máquina y seleccionamos si se desea crear uno o varios archivos para el disco. Se recomienda en un solo archivo ya que el rendimiento de la máquina será óptimo.



La pantalla que se muestra a continuación nos indica un resumen de las características de nuestra máquina virtual. Adicionalmente, es posible realizar modificaciones de acuerdo con nuestras necesidades.



En este apartado podemos cambiar la cantidad de procesadores, así como añadir un adaptador de red o la cantidad de MegaBytes de la memoria RAM que asignaremos.

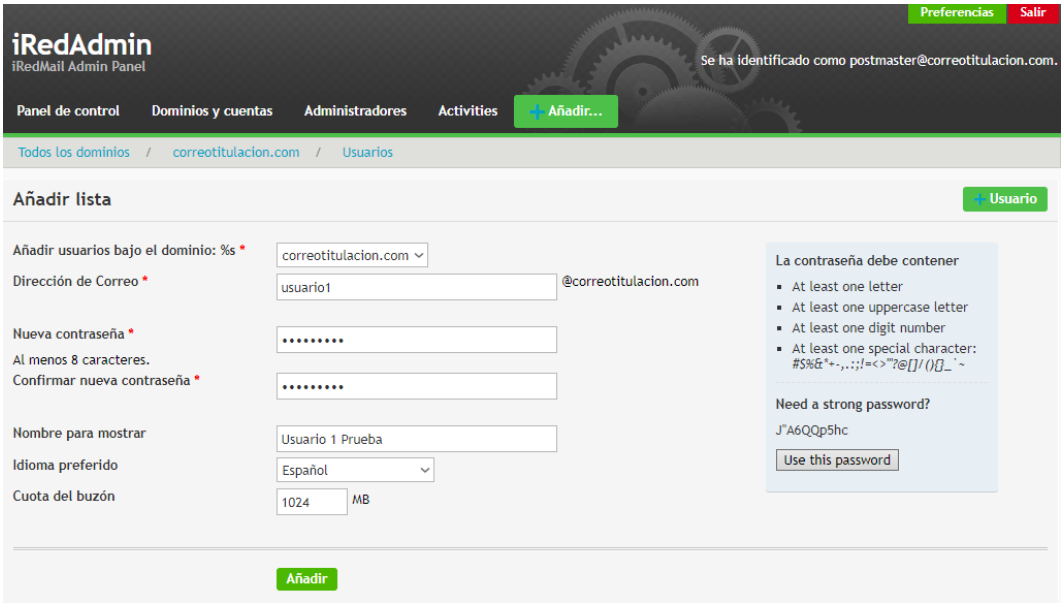


Anexo B: Registro de usuarios en servidor de correo electrónico.

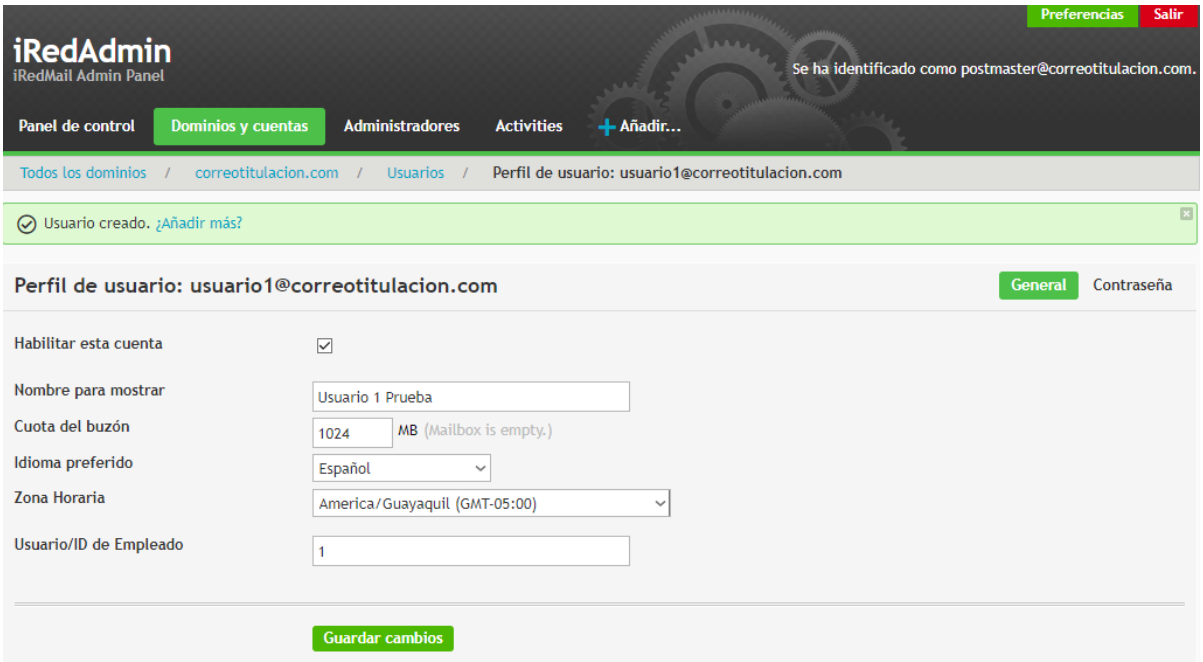
Se puede observar que al iniciar la configuración no se tiene ningún usuario creado a más del *postmaster* que es el administrador; del mismo modo solo tenemos un dominio que es el que creamos por defecto:

Procedemos a añadir usuarios en el apartado añadir:

Procedemos a llenar los campos requeridos y el espacio que dispone el usuario para sus correos electrónicos.

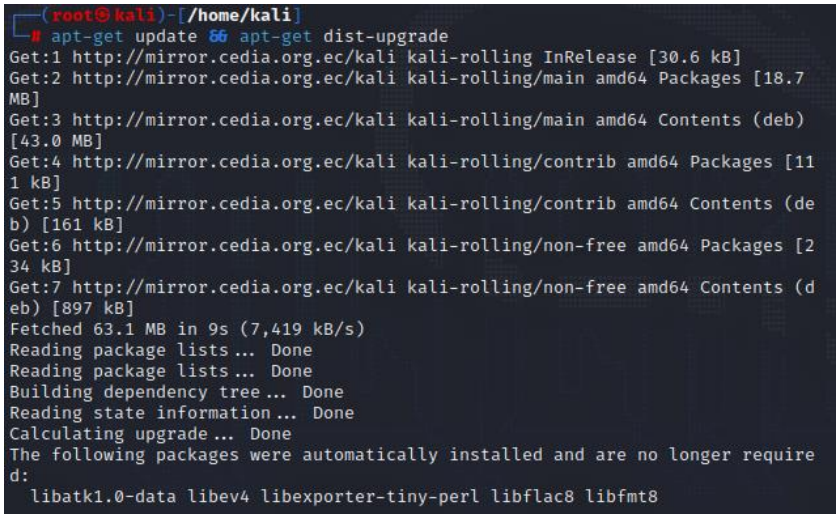


Se procede a configurar el nombre que se desea mostrar para el usuario que se está creando, así como el almacenamiento que contará dicho usuario.

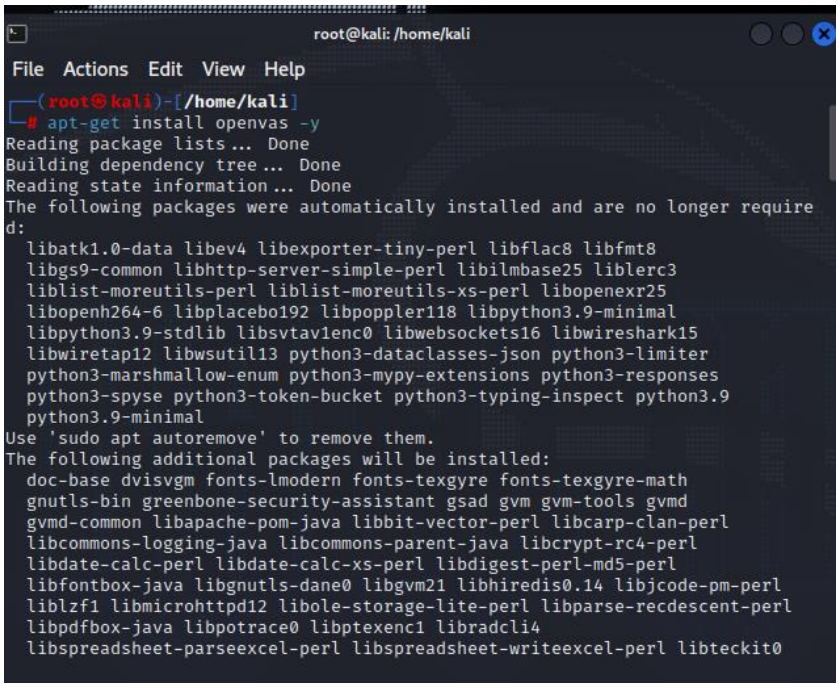


Anexo C: Instalación OpenVAS.

En primer lugar, se requiere actualizar (de ser necesario) el sistema con: *apt-get update && sudo apt-get dist-upgrade*.



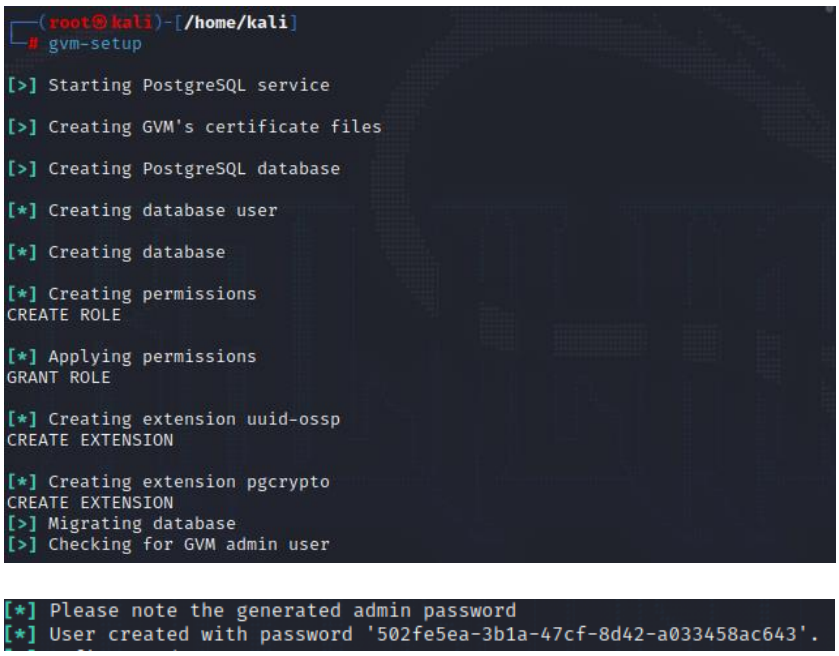
Posteriormente se procede a instalar OpenVAS con el comando: *apt-get install openvas -y*.



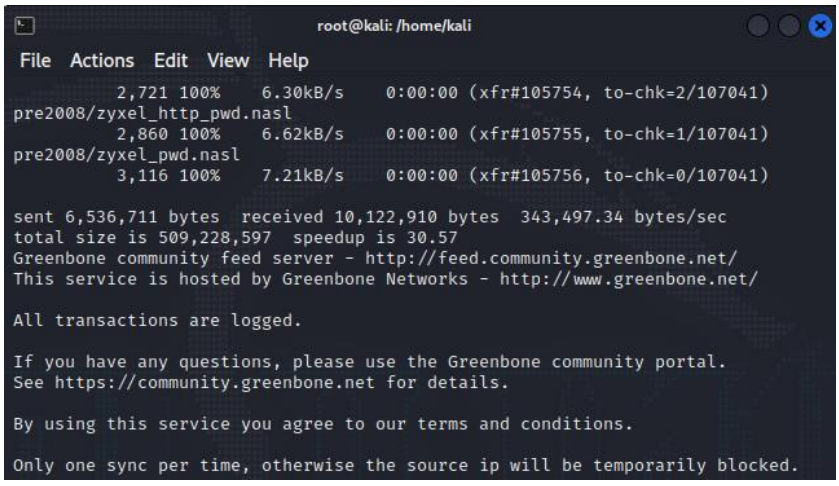
Una vez instalada la herramienta se procede a ejecutar el comando para la configuración de OpenVAS así como para la obtención de las credenciales para el uso de la aplicación: *gvm-setup*.

Usuario: admin

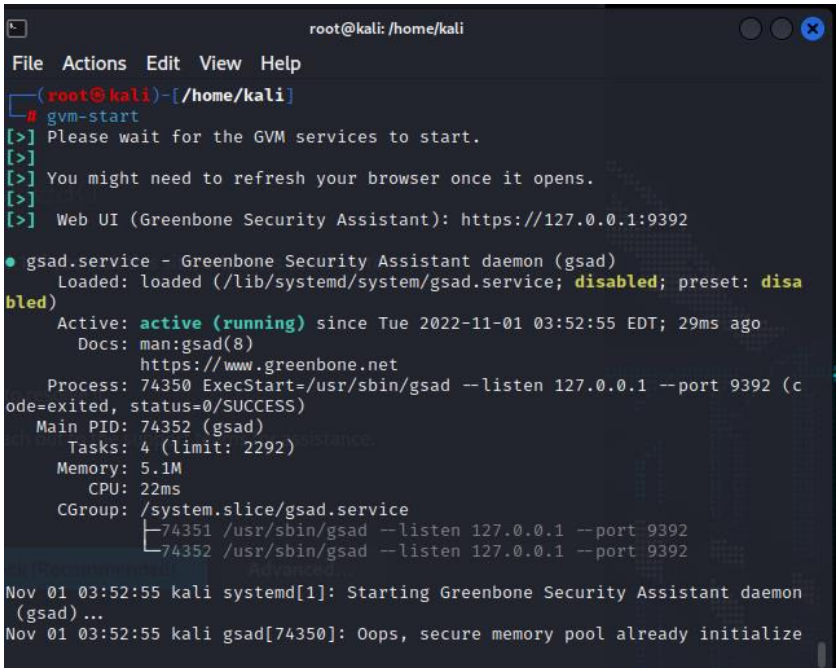
Contraeña: 502fe5ea-3b1a-47cf-8d42-a033458ac643

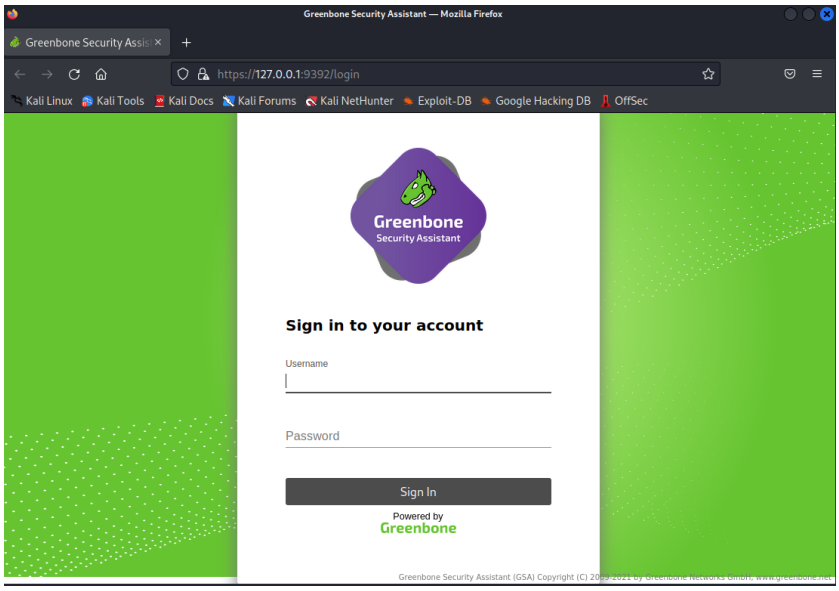


Ya configurado OpenVAS es necesario realizar una actualización de la base de datos de vulenrabildiades y fallos para poder realizar un análisis exitoso: *sudo gvm-feed-update*.



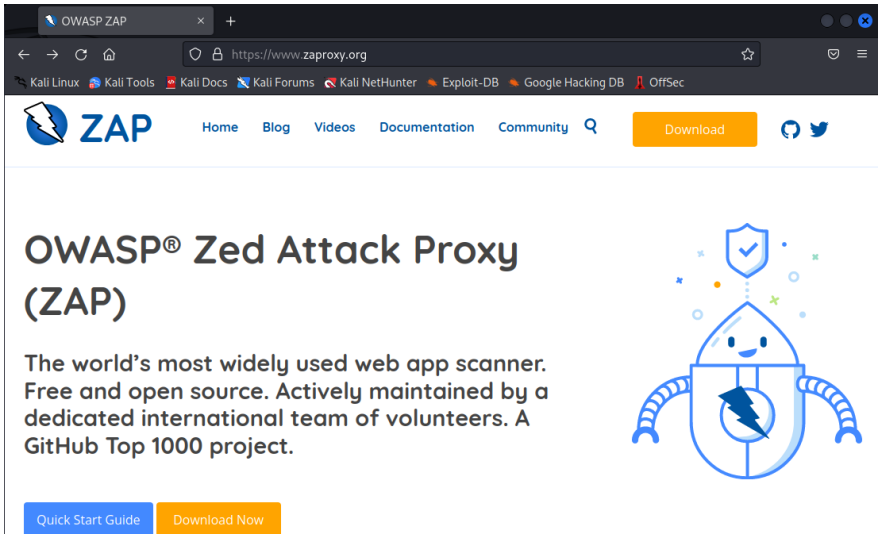
Finalmente procedemos a inicializar los servicios de OpenVAS y de este modo poder acceder mediante el navegador hacia la herramienta e iniciar sesión con las credenciales entregadas previamente: *sudo gvm-start*.



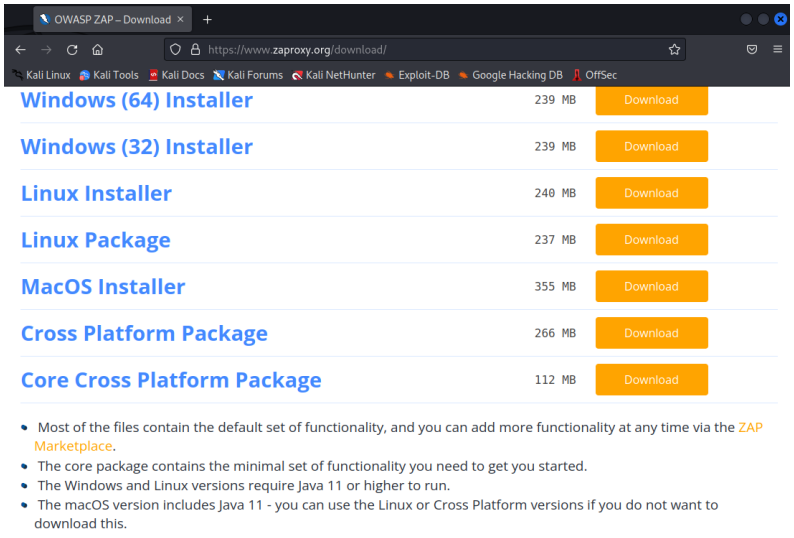


Anexo D: Instalación OWASP-ZAP

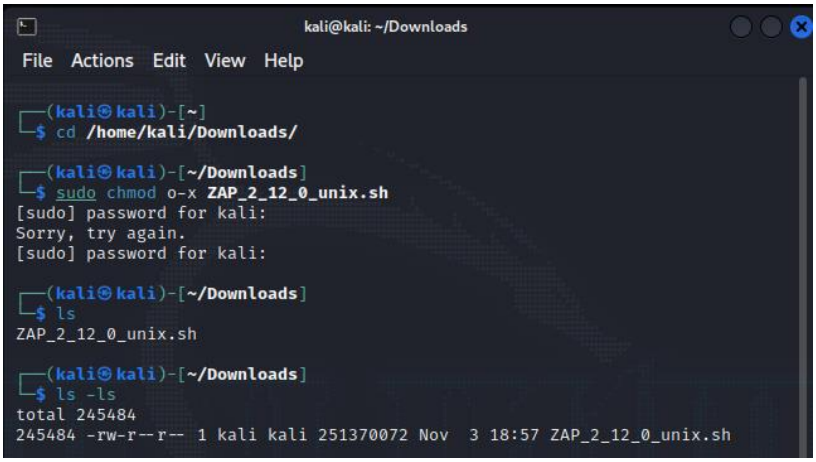
Dirigirse a www.zaproxy.org



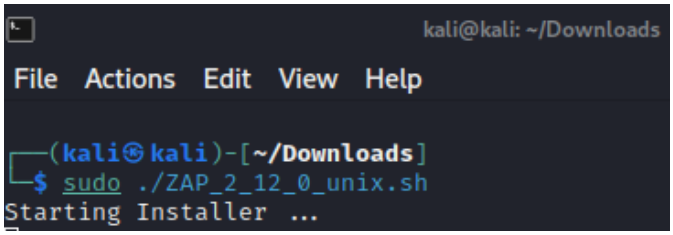
En el apartado de descargas seleccionamos Linux Installer



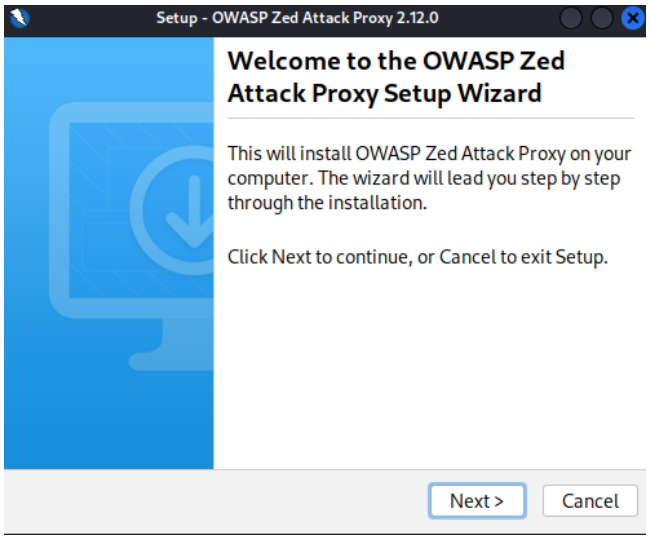
Una vez finalizada la descarga, en una terminal procedemos a dirigirnos a la carpeta de descargas y otorgamos los permisos necesarios al archivo que acabamos de descargar.



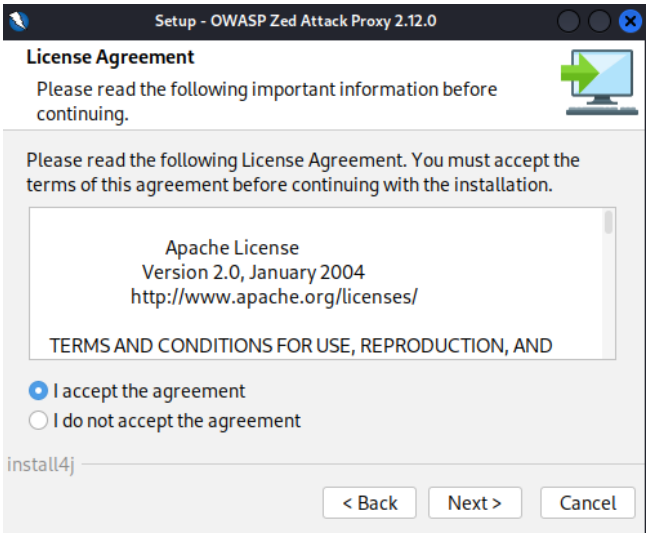
Posteriormente procedemos a ejecutarlo para su instalación.



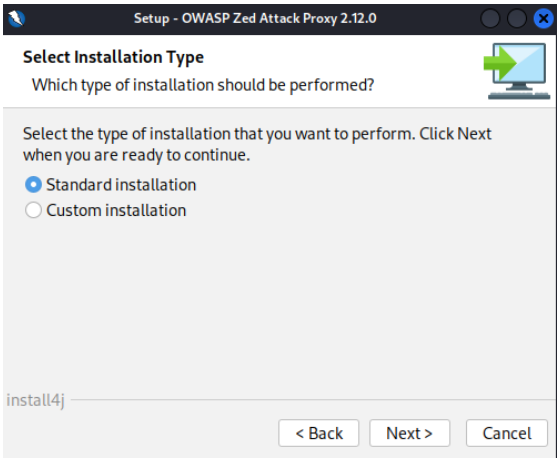
Se desplegará el menú de instalación.



Presionamos en continuar y aceptamos los términos y condiciones.

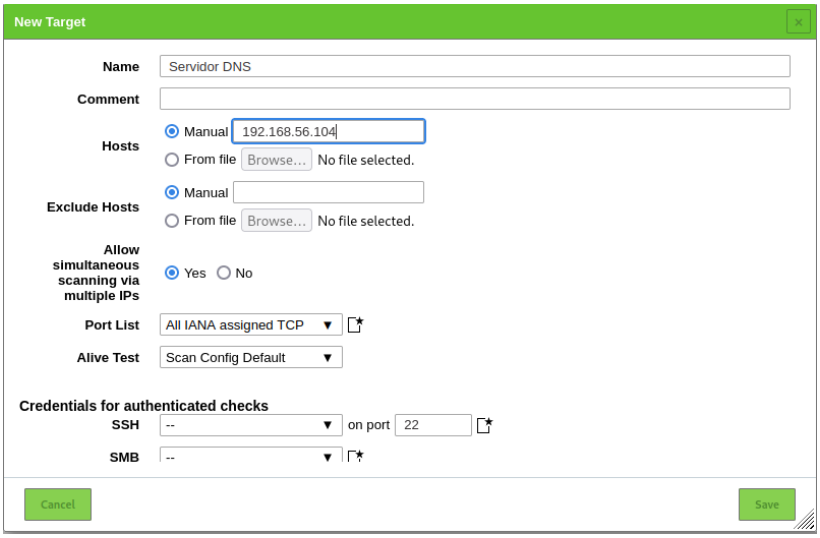


Seleccionamos la instalación estándar y esperamos a que finalice la instalación.



Anexo E: Añadir dispositivos para análisis de Vulnerabilidades en OpenVAS.

Sdsds Añadimos un nuevo “Target” con un nombre y la dirección IP del mismo.

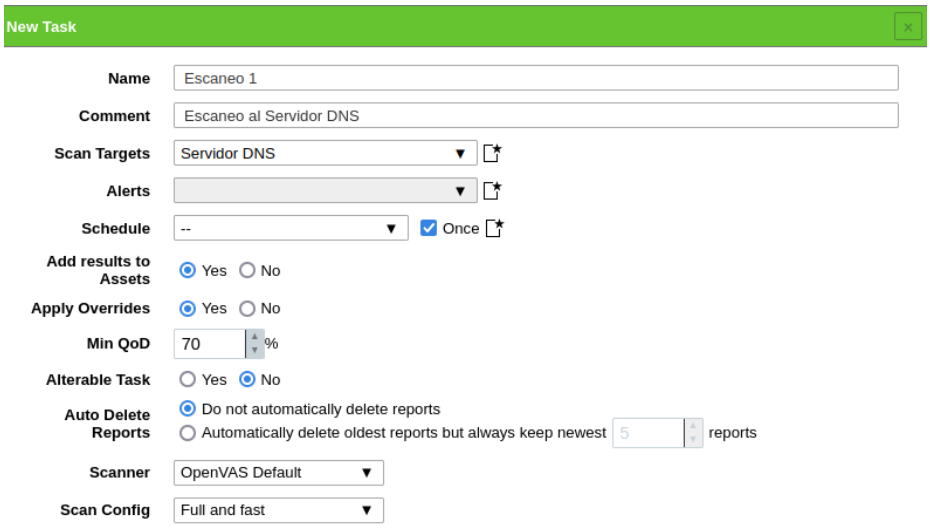


En el apartado de lista de puertos, es posible incluir la lista de puertos que se requieren para realizar un análisis más específico en caso de que ciertos puertos se encuentren en ataque.

Es posible ingresar las credenciales para la conexión SSH del servidor y con ello realizar búsquedas de vulnerabilidades más internas.

Anexo F: Creación de tareas para análisis con la herramienta OpenVAS.

En el apartado de Escáneres seleccionaremos “Tareas” y crearemos una nueva tarea. Se selecciona el objetivo al que se le quiere hacer el ataque. Es posible configurar la frecuencia con la que se requiere que se haga el escaneo.



Para seleccionar el tipo de escaneo se tiene dos opciones: escaneo de vulnerabilidades documentadas o conocidas y escaneo de vulnerabilidades con OpenVAS con pruebas de seguridad. Finalmente, en la configuración del escaneo existen varias opciones, pero se recomienda realizar un escaneo completo para abarcar la mayor cantidad de funcionalidades de la herramienta.