ANÁLISIS DE VULNERABILIDADES AL SERVIDOR DE PRUEBAS DEL DEPARTAMENTO DE SISTEMAS DE LA E.S.E. HOSPITAL MARCO FELIPE AFANADOR DEL MUNICIPIO DE TOCAIMA CUNDINAMARCA GENERANDO LAS RECOMENDACIONES PARA REALIZAR UN PROCESO DE HARDENING

DIEGO FRANCISCO BALLEN LEÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
TOCAIMA
2019

ANÁLISIS DE VULNERABILIDADES AL SERVIDOR DE PRUEBAS DEL DEPARTAMENTO DE SISTEMAS DE LA E.S.E. HOSPITAL MARCO FELIPE AFANADOR DEL MUNICIPIO DE TOCAIMA CUNDINAMARCA GENERANDO LAS RECOMENDACIONES PARA REALIZAR UN PROCESO DE HARDENING

DIEGO FRANCISCO BALLEN LEÓN

Línea de Investigación:

Infraestructura tecnológica y Seguridad enredes

Director

DANNY FERNANDO LEÓN

Lic. en Electrónica, M.Sc. en Ciencias de la Información y las Comunicaciones

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
TOCAIMA
2019

Nota de Aceptación

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

CONTENIDO

INTRODUCCIÓN 9
1.Planteamiento del problema 10
1.1 Antecedentes del problema 11
1. 2 Formulación del problema 11
2. Justificación 12
3. Objetivos 13
3.1Objetivo general 13
3.2Objetivos específicos 13
4. Marco de Referencia 14
4.1 Antecedentes de investigación 14
4.1.1 Historia de las vulnerabilidades 14
4.1.2 Ataques informáticos a través de la historia 16
5. Marco Contextual 18
5.1 E.S.E Hospital Marco Felipe Afanador de Tocaima 18
5.2 Misión 19
5.3 Visión 19
5.4 Política de Tratamiento de información 19
5.4.1 Generalidades 20
5.4.2 disposiciones generales establecidas en la ley 1581 de 2012 para la protección de datos personales 22
5.4.3 deberes del responsable del tratamiento 23
5.4.4 derechos de los titulares 24
5.4.5 políticas 25
6. Marco Teórico 31
6.1 La seguridad de la información 31
6.2 ISO/IEC 27000 32
6.3 SGSI (Sistema de Gestión de Seguridad de la Información) 34
6.4 Nmap para el uso de análisis de vulnerabilidades 36
6.5 Openvas y el análisis de vulnerabilidades 36
7. Marco Conceptual 38

7.1 ¿Que son las vulnerabilidades informáticas? 38
7.2 Tipos de vulnerabilidades informáticas 39
7.3 Herramientas de análisis de vulnerabilidades 43
7.4 KALI LINUX 43
7.5 NMAP Y OPENVAS 44
8. presentación de las herramientas que se van a utilizar 46
8.1 Virtual Box 46
8.2 Kali Linux 47
8. 3 Nmap 48
8.4 Openvas 49
9. Análisis de Vulnerabilidades 50
9.1 Virtual Box 50
9.2 Kali Linux 55
9.2.1 Instalación de OpenVas 61
9.3 Red y Conectividad 65
9.4 Análisis con Nmap 66
9.4.1 Comandos a Utilizar 66
9.4.1.1 Nmap + Ip del Host 67
9.4.1.2 Nmap – Sv 68
9.4.1.3 Nmap - A 69
9.5 Análisis con OpenVas 70
10. Análisis de resultados y recomendaciones para el proceso de hardening 78
10.1 Resultados Nmap 78
10.2 Resultados Openvas 79
Conclusiones 82
Bibliografía 84
Anexos 92

LISTA DE FIGURAS

Figura 1 Virtual Box Logo 46
Figura 2 Kali Linux Logo 47
Figura 3 Nmap Logo 48
Figura 4 OpenVas Logo 49
Figura 5 Servidor de pruebas E.S.E. Hospital Marco Felipe Afanador de Tocaima 50
Figura 6 Página Oficial de Virtual Box 51
Figura 7 Interfaz de Virtual Box 52
Figura 8 Creación de Máquina Virtual Kali Linux 53
Figura 9 Configuración de red Virtual Box 54
Figura 10 Página Oficial de Kali Linux 55
Figura 11 Kali Linux descarga de imagen recomendada 56
Figura 12 Ejecución de Kali Linux en Virtual Box 57
Figura 13 Escritorio de Kali Linux 58
Figura 14 Actualización de los paquetes de Kali Linux por línea de comandos 59
Figura 15 Menú de herramientas de análisis de vulnerabilidades Kali Linux 60
Figura 16 Instalación de OpenVas – 1 61
Figura 17 Instalación de OpenVas – 2 62
Figura 18 Instalación de OpenVas – 3 62
Figura 19 OpenVas en el menú de análisis de vulnerabilidades kali Linux 63
Figura 20 Dirección Ip Servidor de Pruebas 65
Figura 21 Prueba de Ping desde la máquina Virtual 65
Figura 22 Nmap + Ip del Host 67
Figura 23 Nmap –sV ..... **¡Error! Marcador no definido.**
Figura 24 Nmap -A -- parte 1 69
Figura 25 Nmap -A -- Parte 2 70
Figura 26 Análisis con OpenVas 1 ..... **¡Error! Marcador no definido.**

Figura 27 Análisis con OpenVas 2 - interfaz principal..... 72
Figura 28 OpenVas Wizard..... 73
Figura 29 Inicio Análisis Openvas 74
Figura 30 Análisis Terminado Openvas..... 75
Figura 31Vulnerabilidades Encontradas 76
Figura 32 Ejemplo detallado de vulnerabilidad Greenbone..... 77

Lista de Anexos

Anexo 1 Solicitud de permiso aprobada por el gerente del hospital para realizar el análisis de vulnerabilidades 92
Anexo 2 Informe Openvas 93

INTRODUCCIÓN

La tecnología está presente en la mayoría de los ámbitos actuales y cada vez esta emerge con un nuevo avance remplazando o mejorando los procesos de un sistema u organización, para el campo de la salud esto no es la excepción, en la E.S.E. hospital Marco Felipe Afanador de Tocaima desde sus inicios y antes de convertirse en empresa social del estado (E.S.E.) siempre se ha buscado implementar la mejor infraestructura tecnológica posible esto con el fin de generar evolución, eficiencia y eficacia en los procesos.

En este proyecto se analizaran las posibles vulnerabilidades del servidor de pruebas que es el equivalente exacto del servidor central de bases de datos de la E.S.E. Hospital Marco Felipe Afanador de Tocaima Cundinamarca ubicado en el departamento de sistemas, generando el informe de los hallazgos encontrados con las recomendaciones necesarias según el análisis para que el líder de procesos del departamento de sistemas implemente un proceso de Hardening al servidor.

Para el análisis de vulnerabilidades en el servidor de pruebas, usaremos una de las distribuciones de seguridad más conocidas para realizar este tipo de procesos, nos referimos a KALI LINUX esta herramienta basada en DEBIAN gnu/Linux, fue creada para realizar procesos de auditoria y seguridad informática, contando con más de 300 herramientas para realizar diferentes tipos de pruebas, según la versión de la distribución estas se actualizan o reemplazan por versiones mejores, al ser de código abierto es personalizable permitiéndonos agregar herramientas y funcionalidades a la distribución.

Para complementar el análisis usaremos las herramientas NMAP y OPENVAS, documentando todo el proceso hasta la generación de un informe con las recomendaciones necesarias para que el líder de procesos implemente las mejoras y/o cambios pertinentes para asegurar el servidor de pruebas de la institución

1. PLANTEAMIENTO DEL PROBLEMA

Nuestro mundo evoluciona día a día y gracias a la tecnología varios de los ámbitos actuales son remplazados o mejorados mediante varios tipos de sistemas, en las instituciones que prestan servicios de salud esta evolución no es la excepción, en la E.S.E. hospital Marco Felipe Afanador de Tocaima desde sus inicios y antes de convertirse en empresa social del estado (E.S.E.) siempre se ha buscado implementar la mejor infraestructura tecnológica posible esto con el fin de generar mejoras, eficiencia y eficacia en los procesos.

Esta evolución también genera nuevos riesgos y posibles amenazas a la infraestructura, para centrarnos más en el problema nos enfocaremos en los servidores, estos están presentes en casi cualquier tipo de empresa u organización hoy en día volviéndose el corazón de la organización ya que proporcionan servicios de software y demás aplicativos asociados para que la empresa ponga en marcha su producción, la E.S.E. Hospital Marco Felipe Afanador de Tocaima no es la excepción, los servidores ubicados en el rack del departamento de sistemas serán los "sujetos" que vamos a intervenir en este proyecto, para ser más específicos y por obvias razones de seguridad informática e integridad en los procesos de producción de esta institución trabajaremos en el servidor de pruebas que es una copia exacta del servidor de producción principal.

Con el tiempo los cambios de administración de personal y de procesos tanto administrativos como asistenciales deben seguir una trazabilidad para asegurar su éxito; En el departamento de sistemas de esta institución algunos de sus procesos no cuentan con esta trazabilidad o estos simplemente no las generan, aunque no son todos los procesos en este departamento los que no cuentan con documentación y/o trazabilidad, algunos de estos se encuentran desactualizados o jamás se han realizado.

Precisamente al no tener una documentación de estos procedimientos genera de por si una gran problemática debido a que no se sabrá el estado inicial de su infraestructura tecnológica y procesos relacionados, tampoco se conocerán los cambios realizados, sus hallazgos, correcciones, actualizaciones y futuros cambios, y todo este proceso para un nuevo líder o administrador de sistemas se tienen que realizar desde cero o simplemente se continúa y se pierde pensando que todo está bien, en esta institución ninguno de los servidores cuenta con ninguna guía de procesos, o bitácora documentada relacionada al departamento de sistemas en su documentación oficial como el PETI. (Plan estratégico de las tecnologías de la información) o el PNSI (plan de necesidades de sistemas de

información), debido a esto se genera este proyecto con el fin de aportar a esta institución la guía necesaria para la mitigación y corrección de posibles problemas y amenazas informáticas con base en el análisis que se realizara al servidor de pruebas.

1.1 ANTECEDENTES DEL PROBLEMA

No existen antecedentes registrados en la E.S.E. Hospital marco Felipe afanador de Tocaima y su departamento de sistemas, sobre procesos de análisis de vulnerabilidades realizados de forma interna o por medo de terceros, tampoco existen situaciones en donde se hayan presentado ataques de cualquier tipo a la infraestructura informática aprovechando vulnerabilidades en alguno de sus componentes, por lo tal este será el primer proceso de esta naturaleza que se realice a un componente de la infraestructura informática de la institución como lo es su servidor de pruebas.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el análisis de vulnerabilidades al servidor de pruebas del departamento de sistemas de la E.S.E. hospital marco Felipe Afanador del municipio de Tocaima Cundinamarca, y la generación de las recomendaciones para realizar un proceso de Hardening con base en estos resultados, permitirá mejorar los niveles de seguridad de la información en esta institución?

2. JUSTIFICACIÓN

Los ataques informáticos y amenazas como virus o software malintencionado afectan a cualquier componente de una infraestructura informática, estas amenazas siempre estarán presentes no importa el método de protección que se utilice, ya que pueden evolucionar para adaptarse y romper las vulnerabilidades que se generan con el paso de las nuevas tecnologías, es importante que cualquier administrador del sistema, dependencia o departamento con fines informáticos conozcan el estado de su infraestructura (hardware y software), para estar siempre a la vanguardia en equipos y tecnologías de tal manera que se mitiguen o se prevengan vulnerabilidades en la infraestructura desde este perfil tecnológico.

Mediante este proyecto se aportara a esta institución y a su área de sistemas la información pertinente para mitigar posibles vulnerabilidades informáticas que puedan ocasionar fallas críticas en sus procesos productivos, esto por medio de un análisis de vulnerabilidades aplicado a su servidor de pruebas; En algunas empresas se vive en un ambiente de poco seguimiento a los procesos sumándole a esto los cambios administrativos encontramos falencias sistemáticas que abren la puerta a distintos tipos de problemas, observando el área informática, al no conocer al 100% el estado de su infraestructura tecnológica y sus procedimientos esto se volverá fatal a largo plazo para la empresa los servicios prestados ocasionando traumatismo a sus usuarios.

Como ninguna organización está exenta de ser víctima de un ataque o amenaza informática al analizar las posibles vulnerabilidades en sus servidores podemos encontrar información relevante que nos proporcione los medios necesarios para prevenir o mitigar estos riesgos informáticos, el realizar este proceso de análisis en el servidor de pruebas de la E.S.E. Hospital Marco Felipe Afanador de Tocaima, proporcionaremos las sugerencias necesarias para que estas falencias sean revisadas y corregidas por los integrantes de su departamento de sistemas y así prevenir posibles escenarios catastróficos.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un análisis de vulnerabilidades al servidor de pruebas de la E.S.E. Hospital Marco Felipe Afanador del Municipio de Tocaima Cundinamarca generando un informe con las sugerencias para realizar un proceso de Hardening

3.2 OBJETIVOS ESPECÍFICOS

- Plantear las herramientas que se utilizaran para el análisis de vulnerabilidades
- Describir las características de estas herramientas y su uso para análisis de vulnerabilidades
- Ejecutar el análisis de vulnerabilidades con las herramientas propuestas para esta actividad
- Analizar los resultados capturados en el análisis de vulnerabilidades
- Documentar estas vulnerabilidades en un informe detallado
- Entregar el informe detallado junto con una presentación describiendo la importancia del proceso de Hardening al servidor de bases de datos

4. MARCO REFERENCIAL

4.1 ANTECEDENTES DE INVESTIGACIÓN

4.1.1 **Historia de las vulnerabilidades.** El campo de la seguridad Informática ha cambiado en los últimos años inicialmente el objetivo de esta era asegurar un objetivo en específico o aislado, esto se ha evolucionado a la protección general del bien más valioso que puede tener una empresa u organización que es la información, enfocando toda su energía e investigación a fortalecer los procesos de una empresa, las vulnerabilidades informáticas inicialmente en los años 80 y 90 estaban orientadas al control interno, es decir hacia los usuarios, se aseguraba la máquina y el S.O. (sistema operativo), su seguridad era básica y lógica y por lo general se centraban en la protección de los virus informáticos de aquella época.

Pero esta metodología cambio cuando el internet llego al mundo informático, el efecto de globalización que ocasionó a nivel empresarial transformó la seguridad informática y los procesos de fortalecimiento se enfocaron hacia la conectividad o como se denomina el "networking", protegiendo ahora los servidores de aplicaciones informáticas, y el acceso a través de internet por medio de firewalls, con la posibilidad ahora de estar conectados nuevas amenazas y vulnerabilidades que podían ser explotadas surgen debido a que la información vital para la empresa u organización podía ser accesible precisamente gracias a esa conectividad.

La evolución informática no aplica solo para los sistemas también los atacantes aprovechan estos cambios para mejorar sus métodos de ataque, antes de que internet se expandiera como lo ha hecho hoy en día, para un atacante informático o hacker le era más simple acceder a un sitio donde nadie antes había conseguido llegar, o infectar un sistema mediante algún tipo de virus, pero sin ningún tipo de lucro, actualmente los objetivos de los malhechores informáticos han cambiado debido a que se han dado cuenta de lo importante que es la información, cambiando los vectores de ataque al punto de que la mayoría de ataques no se hacen en solitario, ahora existen grupos organizados que aprovechan las vulnerabilidades de los sistemas informáticos para acceder a la información crítica de una empresa, esto por medio de explotación de vulnerabilidades para obtener información muy específica.

Ante estas nuevas amenazas surgen mecanismos de protección mucho más avanzados tales como:

- IDS (Intrusión Detection System). Sistemas de monitorización y detección de accesos no permitidos en una red.

- IPS (Intrusión Prevention System). Sistemas de prevención de intrusión. No solo monitoriza el tráfico para detectar vectores de ataque en una red, sino que el sistema es capaz de bloquearlos.

- Honeypot. equipos aparentemente vulnerables que en realidad no contienen ninguna información sensible de la empresa sino que están diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.

- SIEM (Security Information en Event Management). Sistemas de correlación de eventos y generación de alertas, capaces de integrar diferentes dispositivos, lanzar acciones en función de las alertas, y almacenar los registros para un posterior análisis de los mismos.

Debido a los nuevos métodos de ataque, la adaptabilidad de los atacantes y la importancia de la información crítica para una organización, el concepto de seguridad informática se adapta y transforma, ahora se denomina seguridad de la información con el fin de alinear las inversiones en seguridad de la empresa aportando a sus estrategias de negocio esto por medio del diseño de políticas de seguridad que deben tener en cuenta lo siguiente:

- Localización de la empresa
- Tamaño de la empresa
- Número de sedes
- Condicionantes geográficas
- Cumplimientos legales y normativas vigentes,
- Normas ISO de la empresa, entre otras

Al hablar de evolución de la seguridad, también se debe hablar de integración de la seguridad informática en la seguridad de la información, la seguridad de la información es un concepto más global que define e integra políticas de seguridad en los planes estratégicos, por ello se cuantifican los riesgos, se identifican aquellos más críticos para el negocio de forma continua, se plantean escenarios de crisis y se diseñan planes de continuidad de negocio y recuperación ante desastres, toda esta información, junto con un buen diseño de seguridad y una profunda integración de la seguridad en los planes estratégicos de la empresa de forma constante implicando desde luego a la gerencia y el personal directivo de la empresa, permitirán conocer dónde y cómo utilizar las medidas técnicas de seguridad informática en el marco de la seguridad de la información y sus medidas organizativas.

4.1.2 **Ataques informáticos a través de la historia.** Varios han sido los ataques informáticos que han sucedido alrededor de la historia y algunos han tenido tal magnitud que han dejado su huella, en el 2016 realizaron potentes ataques DDoS (ataque distribuido de denegación de servicio, en español) interrumpieron el servicio de una gran cantidad de sitios web, incluyendo Twitter, Netflix, PayPal, Pinterest y PlayStation Network, entre otros, ese mismo año en junion una hacker bajo el apodo "Peace" se hizo conocido por publicar datos de millones de usuarios de LinkedIn, Tumblr y Myspace, más de medio billón de contraseñas estuvieron disponibles en línea. Según Wired, el listado incluía 167 millones de cuentas de usuarios de LinkedIn, 360 millones de MySpace, 68 millones de Tumblr, 100 millones de la red social rusa VK.com y 71 millones de Twitter, sumando más de 800 millones de cuentas y creciendo. Entre los afectados hubo figuras conocidas como el CEO de Facebook Mark Zuckerberg, los cantantes Katy Perry y Drake y el cofundador de Twitter Biz Stone, entre otros, El nacional.com (2016) "los-incidentes-seguridad-informatica-mas-importantes-del-ultimo-ano"

En 2004, Shawn Carpenter descubrió una serie de "incursiones cibernéticas" por parte de lo que, según diera a conocer el FBI, se trataba de células apoyadas por el gobierno chino. Llamado "Titan Rain", durante el ataque los hackers pudieron infiltrarse a varias redes y ordenadores, incluidos los de la NASA. Considerado uno de los mayores ataques cibernéticos de la historia, en este no sólo se consiguió infiltrar a inteligencia militar y datos clasificados, sino que permitió que otros hackers y entidades de espionaje hallaran la forma de inhabilitar diversas máquinas, Martínez E. (2017) "7 de los ciberataques más famosos de la historia"

Heartbleed no fue un virus, sino un Bug que por error fue escrito en OpenSSL. Esto permitió a los hackers a crear una puerta de entrada hacia diversas bases de datos. Se ha dicho que este es uno de los mayores ciberataques en la historia, pues según algunos reportes sugieren que cerca del 17% de todos los sitios web fueron afectados.

Este ataque permitió que diversos hackers tuvieran acceso a conversaciones privadas sin que los usuarios se percataran, gracias a que implantaron un portal en el sistema para tener acceso en cualquier momento. Pasaron cerca de dos años hasta que el Bug fue finalmente detectado en 2014 por Google Security, Martínez E. (2017) “7 de los ciberataques más famosos de la historia”.

5. MARCO CONTEXTUAL

5.1 E.S.E HOSPITAL MARCO FELIPE AFANADOR DE TOCAIMA

La E.S.E. hospital marco Felipe afanador de Tocaima, es un hospital de primer nivel ubicado en el municipio de Tocaima – Cundinamarca, inicialmente el hospital no tenía este nombre según su historia, su anterior nombre era hospital san Rafael de Tocaima y bajo ordenanza número 9 de noviembre 3 de 1949 de la asamblea del departamento de Cundinamarca el hospital san Rafael de Tocaima toma carácter distrital para todos los efectos de las disposiciones sobre hospitales distritales de beneficencia, 47 años más tarde, por ordenanza 035 de mayo 09 de 1996 de la asamblea de Cundinamarca, se transformó en empresa social del estado (E.S.E.) hospital marco Felipe afanador de Tocaima, de acuerdo a la estructura administrativa del sistema nacional de salud, el hospital pertenece al nivel I ofreciendo algunos servicios de segundo nivel; constituida como categoría especial de entidad pública descentralizada del orden departamental, dotada de personería jurídica, patrimonio propio y autonomía administrativa adscrita a la dirección departamental de seguridad social en salud de Cundinamarca o quien haga sus veces, integrante del sistema general de seguridad social en salud, acatando las disposiciones legales vigentes se ha constituido la junta directiva como máximo ente directivo de la institución.

Como se menciona en la ordenanza 035 este hospital es catalogado como un hospital de primer nivel, pero tiene habilitados servicios se segundo nivel, especialistas y cirugía, pero ¿Qué es primer nivel?, según Redacción El Tiempo. (1997). Recuperado de: https://www.eltiempo.com/archivo/documento/MAM-627858.”A este nivel pertenecen los hospitales locales donde se brinda una atención básica. Solo cuentan con médicos generales para la atención de consultas y no hacen procedimientos quirúrgicos. Eventualmente, prestan servicio de odontología general.”,

Según Clasificacionde (2008). Recuperado de: https://www.clasificacionde.org/hospitales/.”En este nivel, se atiende a la población para la prevención de enfermedades, medicina general, además de poseer aparatos de menor complejidad, generalmente, son llamados, sanatorios, dispensarios o ambulatorios, y atienden necesidades como la odontología, consultas generales, ginecología, atención de urgencias mediana, laboratorio, además, partos no complejos, asimismo, es encargado de la prevención de enfermedades, así como la educación de la población para prevenirlas, por lo tanto, es el encargado de la salud integral de la población y su recuperación”.

La E.S.E. Hospital Marco Felipe Afanador de Tocaima adicionalmente a su clasificación cuenta bajo su cargo 4 sedes más, en el municipio de Apulo, el centro de salud Rafael Reyes, en agua de dios, el centro de salud Johan, en Jerusalén el centro de salud de Jerusalén, y aunque también está a su cargo pero aún no ha entrado en funcionamiento total, el centro de salud de pubenza, todos estos menos el centro de salud de pubenza están interconectados y su infraestructura informática es vigilada y administrada por el departamento de sistemas cuya ubicación central es en Tocaima.

5.2 MISIÓN

Somos la Empresa Social Del Estado Hospital Marco Felipe Afanador de Tocaima, prestador de servicios integrales de salud de baja complejidad, comprometida con la calidad y el medio ambiente, que garantiza la seguridad del paciente con un equipo humanizado para la atención de pacientes, con amplia participación social y de rentabilidad con la comunidad urbana y rural de su área de influencia.

5.3 VISIÓN

Para el año 2020 la ESE Hospital Marco Felipe Afanador de Tocaima, se posicionara como un empresa líder de Atención Primaria en Salud (APS), seremos una organización modelo en el cuidado y restablecimiento de la salud, alineada con nuestras tradiciones, manteniendo la excelencia en la calidad de atención y respeto por la dignidad de las personas, por medio de un Sistema de Gestión de Calidad que permita el mejoramiento continuo a través de alianzas estratégicas con los diferentes actores del sistema de seguridad social en salud, buscando la satisfacción del cliente interno y externo, generando impacto social y ambiental.

5.4 POLÍTICA DE TRATAMIENTO DE INFORMACIÓN

Es importante para este proyecto conocer la política de tratamiento de información vigente de la E.S.E. Hospital Marco Felipe Afanador de Tocaima que es la siguiente según su página oficial http://www.hmfa-tocaima-cundinamarca.gov.co/

5.4.1 Generalidades. Estos datos pueden almacenarse en cualquier soporte físico o electrónico y ser tratados de forma manual o automatizada.

La Ley 1266 de 2008 define los siguientes tipos de datos de carácter personal:

- **Dato privado:** "Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular".

- **Dato semiprivado:** "Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV" de la Ley 1266.

- **Dato público:** "Es el dato calificado como tal según los mandatos de la Ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados", de conformidad con la Ley 1266 de 2008. "Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas".

Adicionalmente, la Ley 1581 de 2012 establece las siguientes categorías especiales de datos personales:

- **Datos sensibles:** Son "aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos".

La Ley 1581 de 2012 prohíbe el tratamiento de datos sensibles con excepción de los siguientes casos: (i) cuando el Titular otorga su consentimiento, (ii) el Tratamiento es necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado, (iii) el tratamiento es efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad, (iv) el Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y (v) el Tratamiento tenga una finalidad histórica, estadística o científica, en este último caso deben adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

- **Datos personales de los niños, niñas y adolescentes:** Se debe tener en cuenta que aunque la Ley 1581 de 2012 prohíbe el tratamiento de los datos personales de los niños, niñas y adolescentes, salvo aquellos que por su naturaleza son públicos, la Corte Constitucional precisó que independientemente de la naturaleza del dato, se puede realizar el tratamiento de éstos "siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, niñas y adolescentes y se asegure sin excepción alguna el respeto a sus derechos prevalentes".

También la ley define los siguientes roles:

a) **Responsable de Tratamiento:** "Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos". La E.S.E. Hospital Marco Felipe Afanador, de acuerdo con la ley es Responsable de Tratamiento de datos personales contenidos en sus bases de datos,

b) **Encargado del Tratamiento:** "Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento". La E.S.E. Hospital Marco Felipe Afanador podrá realizar el tratamiento de sus datos personales a través de Encargados siempre y cuando este proceso sea necesario.

Adicionalmente, para este documento se incluyen los siguientes roles.

c) **Administradores de bases de datos personales:** Funcionarios o Encargados que tienen a cargo el tratamiento a una o más bases de datos que tiene información personal.

5.4.2 Disposiciones generales establecidas en la ley 1581 de 2012 para la protección de datos personales. La Ley 1581 de 2012 desarrolla el derecho constitucional a conocer, actualizar y rectificar la información recogida en bases de datos y los demás derechos, libertades y garantías a que se refieren los artículos 15 y 20 de la Constitución (derecho a la intimidad y derecho a la información, respectivamente).

La citada ley se aplica a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por parte de entidades públicas o privadas.

Considerando el modo de conservación de una base de datos, se puede distinguir entre bases de datos automatizadas y bases de datos manuales o archivos.

Las bases de datos automatizadas son aquellas que se almacenan y administran con la ayuda de herramientas informáticas.

Las bases de datos manuales o archivos son aquellas cuya información se encuentra organizada y almacenada de manera física, como las fichas de pedidos a proveedores que contengan información personal relativa al proveedor, como nombre, identificación, números de teléfono, correo electrónico, etc.

La ley exceptúa del régimen de protección (i) los archivos y las bases de datos pertenecientes al ámbito personal o doméstico; (ii) los que tienen por finalidad la seguridad y la defensa nacionales, la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo, (iii) los que tengan como fin y contengan información de inteligencia y contrainteligencia, (iv) los de información periodística y otros contenidos editoriales, (v) los regulados por la Ley 1266 de 2008 (información financiera y crediticia, comercial, de servicios y proveniente de terceros países) y (vi) los regulados por la Ley 79 de 1993 (sobre censos de población y vivienda).

5.4.3 Deberes del responsable del tratamiento. El Responsable del Tratamiento ha sido definido por la Ley 1581 de 2012 como la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento de los datos.

La E.S.E. Hospital Marco Felipe Afanador de Tocaima, además de ser la autoridad de protección de datos personales tiene la calidad de Responsable del Tratamiento frente a las bases de datos creadas por la entidad.

Son deberes de los Responsables del Tratamiento y, por consiguiente, de la E.S.E. Hospital Marco Felipe Afanador de Tocaima los establecidos en el artículo 17 de la Ley 1581 de 2012:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Solicitar y conservar, en las condiciones previstas en la citada ley, copia de la respectiva autorización otorgada por el Titular.
c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la citada ley.
i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
j) Tramitar las consultas y reclamos formulados en los términos señalados en la citada ley.

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la citada ley y en especial, para la atención de consultas y reclamos.
l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
m) Informar a solicitud del Titular sobre el uso dado a sus datos.
n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio".

5.4.4 Derechos de los titulares. La Ley 1581 de 2012 establece que los Titulares de los datos personales tendrán los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la citada ley.
c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la citada ley y las demás normas que la modifiquen, adicionen o complementen.
e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la ley y a la Constitución.
f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Adicionalmente, el Decreto reglamentario 1377 de 2013 define que los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.

5.4.5 Políticas. Se establecen las siguientes directrices generales:

Primero: Cumplir con toda la normatividad legal vigente colombiana que dicte disposiciones para la protección de datos personales.

Segundo: Cumplir con la ley de protección de datos personales de acuerdo con lo contemplado en el Código de Ética y Buen Gobierno de la E.S.E. Hospital Marco Felipe Afanador.

Tercero: Los Servidores deben acogerse a las inhabilidades, impedimentos, incompatibilidades y conflicto de intereses contemplados en la Ley 734 de 2002 (Código Disciplinario Único, capitulo cuarto) para el tratamiento de Datos Personales.

Políticas específicas relacionadas con el tratamiento de Datos Personales:

a) La E.S.E. Hospital Marco Felipe Afanador realiza el tratamiento de Datos Personales en ejercicio propio de sus funciones legales y para el efecto no requiere la autorización previa, expresa e informada del Titular. Sin embargo, cuando no corresponda a sus funciones deberá obtener la autorización por medio de un documento físico, electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato que permita su posterior consulta a fin de constatar de forma inequívoca que sin el consentimiento del titular los datos nunca hubieran sido capturados y almacenados en medios electrónicos o físicos. Así mismo se podrá obtener por medio de conductas claras e inequívocas del Titular que permitan concluir de una manera razonable que este otorgó su consentimiento para el manejo de sus Datos Personales.

b) La E.S.E. Hospital Marco Felipe Afanador solicitará la autorización a los Titulares de los datos personales y mantendrá las pruebas de ésta, cuando en virtud de las funciones de promoción, divulgación y capacitación, realice invitaciones a charlas, conferencias o eventos que impliquen el Tratamiento de Datos Personales con una finalidad diferente para la cual fueron recolectados inicialmente.

c) En consecuencia, toda labor de tratamiento de Datos Personales realizada en la E.S.E. Hospital Marco Felipe Afanador deberá corresponder al ejercicio de sus funciones legales o a las finalidades mencionadas en la autorización otorgada por el Titular, cuando la situación así lo amerite. De manera particular, las principales finalidades para el tratamiento de Datos Personales que corresponde a la E.S.E. Hospital Marco Felipe Afanador desarrollar en ejercicio de sus funciones legales se relacionan con los siguientes tramites:

- Propiedad industrial
- Protección al consumidor
- Control y verificación de reglamentos técnicos y metrología legal
- Protección de la competencia
- Vigilancia de las cámaras de comercio
- Protección de datos personales
- Asuntos jurisdiccionales

d) El Dato Personal sometido a Tratamiento deberá ser veraz, completo, exacto, actualizado, comprobable y comprensible. La E.S.E. Hospital Marco Felipe Afanador mantendrá la información bajo estas características siempre y cuando el titular informe oportunamente sus novedades.

e) Los Datos Personales solo serán Tratados por aquellos Funcionarios de la E.S.E. Hospital Marco Felipe Afanador que cuenten con el permiso para ello, o quienes dentro de sus funciones tengan a cargo la realización de tales actividades o por los Encargados.

f) La E.S.E. Hospital Marco Felipe Afanador autorizará expresamente a los Administradores de las bases de datos para realizar el tratamiento solicitado por el Titular de la información.

g) En la E.S.E. Hospital Marco Felipe Afanador no hará disponibles Datos Personales para su acceso a través de Internet u otros medios masivos de comunicación, a menos que se trate de información pública o que se establezcan medidas técnicas que permitan controlar el acceso y restringirlo solo a las personas autorizadas por ley o por el titular.

h) Todo Dato Personal que no sea Dato Público se tratará por la E.S.E. Hospital Marco Felipe Afanador como confidencial, aun cuando la relación contractual o el vínculo entre el Titular del Dato Personal y la E.S.E. haya finalizado. A la terminación de dicho vínculo, tales Datos Personales deben continuar siendo Tratados de acuerdo con lo dispuesto por el Manual de Archivo y Retención Documental.

i) Cada área de la E.S.E. Hospital Marco Felipe Afanador debe evaluar la pertinencia de anonimizar los actos administrativos y/o documentos de carácter público que contengan datos personales, para su publicación.

j) El Titular, directamente o a través de las personas debidamente autorizadas, podrá consultar sus Datos Personales en todo momento y especialmente cada vez que existan modificaciones en las Políticas de Tratamiento de la información.

k) La E.S.E. Hospital Marco Felipe Afanador de Tocaima, suministrará, actualizará, ratificará o suprimirá los Datos Personales a solicitud del Titular para corregir información parcial, inexacta, incompleta, fraccionada que induzca al error o aquella que haya sido tratada previa a la vigencia de la ley y que no tenga autorización o sea prohibida.

l) Cuando le sea solicitada información, ya sea mediante una petición, consulta o reclamo por parte del Titular, sobre la manera como son utilizados sus Datos Personales, la E.S.E. Hospital Marco Felipe Afanador de Tocaima deberá entregar dicha información.

m) A solicitud del Titular y cuando no tenga ningún deber legal o contractual de permanecer en las bases de datos de la E.S.E. Hospital Marco Felipe Afanador de Tocaima, los Datos Personales deberán ser eliminados. En caso de proceder una revocatoria de tipo parcial de la autorización para el Tratamiento de Datos Personales para algunas de las finalidades la E.S.E. Hospital Marco Felipe Afanador de Tocaima, podrá seguir utilizando los datos para las demás finalidades respecto de las cuales no proceda dicha revocatoria.

n) Las políticas establecidas por la E.S.E. Hospital Marco Felipe Afanador de Tocaima, respecto al tratamiento de Datos Personales podrán ser modificadas en cualquier momento. Toda modificación se realizará con apego a la normatividad legal vigente, y las mismas entrarán en vigencia y tendrán efectos desde su publicación a través de los mecanismos dispuestos por la E.S.E. Hospital Marco Felipe Afanador de Tocaima, para que los titulares conozcan la política de tratamiento de la información y los cambios que se produzcan en ella.

o) Los Datos Personales solo podrán ser tratados durante el tiempo y en la medida que la finalidad de su tratamiento lo justifique.

p) La E.S.E. Hospital Marco Felipe Afanador de Tocaima será más rigurosa en la aplicación de las políticas de tratamiento de la información cuando se trate del uso de datos personales de los niños, niñas y adolescentes asegurando la protección de sus derechos fundamentales.

q) La E.S.E. Hospital Marco Felipe Afanador de Tocaima podrá intercambiar información de Datos Personales con autoridades gubernamentales o públicas tales como autoridades administrativas, de impuestos, organismos de investigación y autoridades judiciales, cuando la soliciten en ejercicio de sus funciones.

r) Los Datos Personales sujetos a tratamiento deberán ser manejados proveyendo para ello todas las medidas tanto humanas como técnicas para su protección, brindando la seguridad de que ésta no pueda ser copiada, adulterada, eliminada, consultada o de alguna manera utilizada sin autorización o para uso fraudulento.

s) Cuando finalice alguna de la labores de tratamiento de Datos Personales por los Servidores, contratistas o Encargados del tratamiento, y aun después de finalizado su vínculo o relación contractual con la E.S.E. Hospital Marco Felipe Afanador de Tocaima, éstos están obligados a mantener la reserva de la información de acuerdo con la normatividad vigente en la materia.

t) La E.S.E. Hospital Marco Felipe Afanador de Tocaima divulgará en sus servidores, contratistas y terceros encargados del tratamiento las obligaciones que tienen en relación con el tratamiento de Datos Personales mediante campañas y actividades de orden pedagógico.

u) La E.S.E. Hospital Marco Felipe Afanador de Tocaima no realizará transferencia de información relacionada con Datos Personales a países que no cuenten con los niveles adecuados de protección de datos, de acuerdo con los estándares que estén fijados en la misma Superintendencia.

v) El Titular de los datos personales puede ejercer, principalmente, sus derechos mediante la presentación de consultas y reclamos ante la E.S.E. Hospital Marco Felipe Afanador de Tocaima, en su sede cuyo domicilio es la carrera 10 No. 5 – 64 y por el correo electrónico htocaima@cundinamarca.gov.co

w) Cuando exista un Encargado del Tratamiento de Información de Datos Personales, la E.S.E. Hospital Marco Felipe Afanador de Tocaima deberá garantizar que la información que le suministra sea veraz, completa, exacta, actualizada, comprobable y comprensible. Adicionalmente le comunicará de manera oportuna todas las novedades a que haya lugar para que la información siempre se mantenga actualizada.

x) En el caso de existir un Encargado del Tratamiento de información de Datos Personales, la E.S.E. Hospital Marco Felipe Afanador de Tocaima suministrará según el caso, información de Datos Personales únicamente cuyo Tratamiento realice en virtud de sus funciones legales y cuando excepcionalmente éstas no apliquen, con la autorización del Titular.

La E.S.E. Hospital Marco Felipe Afanador de Tocaima Informará al Encargado del Tratamiento de información de Datos Personales, de existir uno, cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

6. MARCO TEÓRICO

6.1 LA SEGURIDAD DE LA INFORMACIÓN

Muchas son las definiciones de la seguridad de la información por ejemplo “La seguridad de la información engloba un conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una institución y asegurar que no salgan de ese sistema establecido por la empresa.” “seguridad-de-la-información-un-conocimiento-imprescindible” (2015). Debido a esto es importante para las organizaciones proteger su información
para asegurar que esté disponible cuando se necesite, que sea fiable y que su distribución esté controlada.

Para una empresa controlar la cantidad de información que maneja puede ser un tema complejo ya que este crece de manera exponencial, dificultando algunas veces los procesos para su protección, la seguridad de los sistemas de información de una organización es una metodología que debe tener cierta continuidad y debe evolucionar con los avances tecnológicos es decir estas a la vanguardia con la tecnología esto permite a la organización cumplir con todos sus objetivos de negocio o misión institucional.

La seguridad de la información en cualquiera de sus ámbitos cuenta con objetivos propios que deben ser seguidos para asegurar su efectividad, los objetivos son los siguientes:

Disponibilidad: esta hace referencia al uso autorizado de la información y es un requisito necesario para garantizar que el sistema trabaje puntualmente y no deniegue el servicio a ningún usuario autorizado, las medidas de disponibilidad protegen al sistema contra determinados problemas como los intentos deliberados o accidentales de realizar un borrado no autorizado de datos o de causar cualquier tipo de denegación del servicio.

***Integridad**:* garantiza que la información del sistema no haya sido alterada por usuarios no autorizados, evitando la pérdida de consistencia, en un sistema de información podemos encontrar dos tipos de integridad:

- ***Integridad de datos***. garantiza que los datos no hayan sido alterados de forma no autorizada, mientras se procesaban, se almacenaban o se transmitían.

- ***Integridad del sistema***. Es la cualidad que posee un sistema cuando realiza la función deseada, de manera no deteriorada y libre de manipulación no autorizada. La integridad, normalmente, es el objetivo de seguridad más importante después de la disponibilidad.

***Confidencialidad**:* mantiene la información privada o secreta a la cual no pueden tener acceso personal que no esté autorizado, la confidencialidad se aplica a los datos almacenados durante su procesamiento, mientras se transmite y se encuentran en tránsito.

6.2 ISO/IEC 27000

Según ISO27000.ES [Consulta: 10 de mayo del 2019] disponible en: http://www.iso27000.es/iso27000.html la ISO/IEC 27000 son "un conjunto de estándares desarrollados o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña."[1] Publicada el 15 de Octubre de 2005, es la norma principal de la serie que contiene los requisitos del sistema de gestión de seguridad de la información dentro de la familia de la ISO 27000 podemos encontrar los siguientes estándares

27002: guía a las organizaciones en el desarrollo de sus SGSI, de igual forma no es obligatoria la implementación de todos los controles enumerados en dicho en ella pero la

organización deberá argumentar la no aplicabilidad de los mismos en resumen la 27002 describe las buenas prácticas, los objetivos de control y controles recomendables en cuanto a seguridad de la información, esta no es certificable y en su última versión contiene 35 objetivos de control y 114 controles, agrupados en 14 dominios (ISO27000.es, 2012)

27003: Consiste en la guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases (ISO27000.es, 2012)

27004: Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA dominios (ISO27000.es, 2012)

1, iso27000.es Serie 27000, Documentación publicada hasta el momento por ISO directamente relacionada con los requisitos de la norma ISO/IEC 27001., 2012

27005: establece las directrices para la gestión del riesgo en la seguridad de la información, apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos (ISO27000.es, 2012)

27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. (ISO27000.es, 2012)

27007: Consiste en una guía de auditoría de un SGSI. (ISO27000.es, 2012)

27011: consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones). (ISO27000.es, 2012)

27031: guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones. (ISO27000.es, 2012)

27032: Consiste en una guía relativa a la ciberseguridad. (ISO27000.es, 2012)

27033: norma que se divide en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante Gateway, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y remuneración de ISO 18028. (ISO27000.es, 2012)

27034: Consiste en una guía de seguridad en aplicaciones. (ISO27000.es, 2012)

27799: Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. (ISO27000.es, 2012)

6.3 SGSI (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN)

Según, FIRMA-E [Sitio web]. [Consulta: 10 de mayo del 2019] disponible en: https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/, un SGSI es "Un conjunto de políticas de administración de la información" [2] en pocas palabras es un proceso sistémico y documentado y conocido por toda la empresa, para la gestión de la seguridad de la información en una organización asegurando siempre los 3 pilares de la seguridad de la información vistos anteriormente "confidencialidad, integridad y disponibilidad" además de todos los sistemas implicados en el tratamiento dentro de la organización.

Según, FIRMA-E [Sitio web]. [Consulta: 10 de mayo del 2019] disponible en: https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/ "La información, junto a los procesos y los sistemas que hacen uso de ella,

son activos demasiado importantes para la empresa" [3], y el SGSI garantizando los 3 pilares fundamentales de la seguridad de la información garantiza par la organización mantener los niveles de competitividad, conformidad, rentabilidad e imagen de la misma, y así conseguir los objetivos empresariales.

Como bien se mención, las empresas y los sistemas de información se encuentran expuestos a un número cada vez más elevado de amenazas que aprovechan cualquier tipo de vulnerabilidad y así cazar los activos más críticos de información cualquier tipo de ataque informático como espionajes, vandalismo, los virus informáticos son ejemplos muy comunes y conocidos, pero también se deben asumir riesgos como incidentes de seguridad que pueden ser causados voluntariamente o involuntariamente dentro de la propia empresa o los que son provocados de forma accidental por catástrofes naturales. (pmg-ssi.com, 2015)

_____

[2], firma-e.com Serie 27000, ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información, 2013

[3], firma-e.com Serie 27000, ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información?, 2013

El cumplimiento de la legislación, la adaptación dinámica la protección adecuada de los objetivos de negocio para obtener el máximo beneficio son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad para la gestión de las empresas a nivel de seguridad de la información, un SGSI tiene guía en los procedimientos en la planificación e implementación de los controles de seguridad que se basan en una evaluación de riesgos y en una medición de la eficiencia de los mismos.

Los beneficios que una empresa u organización adquieren cuando implementa un SGSI son los siguientes:

- Establecer una metodología de Gestión de la Seguridad estructurada y clara.
- Reducir el riesgo de pérdida, robo o corrupción de la información sensible.
- Los clientes tienen acceso a la información mediante medidas de seguridad.
- Los riesgos y los controles son continuamente revisados.
- Se garantiza la confianza de los clientes y los socios de la organización.

- Las auditorías externas ayudan de forma cíclica a identificar las debilidades del SGSI y las áreas que se deben mejorar.
- Facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras un incidente grave.
- Cumple con la legislación vigente sobre información personal, propiedad intelectual y otras.
- La imagen de la organización a nivel internacional mejora.
- Aumenta la confianza y las reglas claras para las personas de la empresa.
- Reduce los costes y la mejora de los procesos y el servicio.
- Se incrementa la motivación y la satisfacción del personal.
- Aumenta la seguridad en base la gestión de procesos en lugar de una compra sistemática de productos y tecnologías. (pmg-ssi.com, 2015)

6.4 NMAP PARA EL USO DE ANÁLISIS DE VULNERABILIDADES

Nmap es una herramienta versátil para el escaneo de vulnerabilidades de una red, este tipo de procesos puede generar gran cantidad de tráfico, pudiendo ocasionar situaciones de negación de servicio en dispositivos de red. NMAP mediante su característica denominada NSE (Nmap Scripting Engine), cual permite escribir y compartir scripts sencillos para automatizar una amplia diversidad de tareas de red y así poder escanear la red rápidamente lo que permite identificar los sistemas vulnerables antes cualquier atacante puede hacerlo. (Caballero, 2015)

El equipo de desarrollo de Nmap lanzo una versión de Nmap 7.70, incorporado varias mejoras en la detección de servicios de un determinado equipo, así como la detección del sistema operativo utilizado por el equipo analizado añadiendo la funcionalidad NSE antes mencionada para el análisis de vulnerabilidades

Para sistemas operativos Windows, se actualizo el driver Npcap, garantizando un mayor rendimiento y estabilidad, con esta nueva versión se integran fingerprints para la detección de servicios en la máquina escaneada, incluyendo la versión de dicho servicio, permitiendo realizar auditorías específicas a esos servicios descubiertos y así poder intentar explotar una vulnerabilidad. (Nmap.org, 2018)

6.5 OPENVAS Y EL ANÁLISIS DE VULNERABILIDADES

Según Mendoza M. (2014) de welivesecurity.com Openvas "se trata de un *framework* que tiene como base servicios y herramientas para la evaluación de vulnerabilidades y puede utilizarse de forma individual o como parte del conjunto de herramientas de seguridad incluidas en OSSIM (Open Source Security Information Management)"

A través de las interfaces que openvas ofrece se interactúa con los servicios: OpenVAS Manager y OpenVAS Scanner, este gestor o manager es el servicio que lleva a cabo tareas como el filtrado o clasificación de los resultados del análisis, control de las bases de datos que contienen la configuración o los resultados de la exploración y la administración de los usuarios, incluyendo grupos y roles.

Por otra parte el escáner ejecuta las denominadas los test de las vulnerabiliades o los NVT (Network Vulnerability Test), es decir, las pruebas de vulnerabilidades de red, conformadas por rutinas que comprueban la presencia de un problema de seguridad específico conocido o potencial en los sistemas. Las NVT se agrupan en familias de pruebas similares, por lo que la selección de las familias y/o NVT individuales es parte de la configuración de escaneo.

El proyecto OpenVAS mantiene una colección de NVT (OpenVAS NVT Feed) que crece constantemente y que actualiza los registros semanalmente. Los equipos instalados con OpenVAS se sincronizan con los servidores para actualizar las pruebas de vulnerabilidades. (openvas.org, 2018)

7. MARCO CONCEPTUAL

7.1 ¿QUE SON LAS VULNERABILIDADES INFORMÁTICAS?

Según SIGNIFICADOS.COM [Sitio web]. [Consulta: 10 de mayo del 2019], disponible en: https://www.significados.com/vulnerabilidad/, una vulnerabilidad es "el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes, sean ellos desastres naturales, desigualdades económicas, políticas, sociales o culturales." [4], pero exactamente una vulnerabilidad informática es el producto de fallos producidos por el mal diseño de un software pero también puede ser causada por las limitaciones propias de la tecnología para la que fue diseñado, pero con el paso de los años, los errores de programación han ido disminuyendo en gran parte a que los nuevos lenguajes de programación son más flexibles.

Pero aun así todavía podemos encontrar con algunos de estos errores cuando ejecutamos un programa, aún los desarrolladores y fabricantes más prestigiosos del mercado pueden incluir en sus programas errores que sus ingenieros van parcheando con actualizaciones a medida que son descubiertos o denunciados por sus usuarios.

Esto se puede ver a menudo en sistemas operativos como Microsoft Windows o Android, navegadores como Firefox, Internet Explorer o Chrome, páginas que se creían a prueba de fallas como Facebook o YouTube, entre otros, las vulnerabilidades informáticas son un problema de nunca acabar debido a que no pasa una época en donde no exista o se haga pública una falla o problema de seguridad informática, por lo general existe competencias para revelar y descubrir vulnerabilidades entre fabricantes y desarrolladores de tecnología a su vez esto se vuelve un problema para los usuarios, debido que al quedar expuesta la vulnerabilidad tan abiertamente, esta información es aprovechado por hackers y ciberdelincuentes.

4, sifnigicados.com Serie 27000, significado o definición de vulnerabilidad, 2018

7.2 TIPOS DE VULNERABILIDADES INFORMÁTICAS

Las vulnerabilidades es un tema fundamental que debe estar presente en los espacios de seguridad de la información de una empresa u organización dejar este tema desactualizado o no tomarlo en serio no puede traer una buena cantidad de peligros, y aunque no todas las organizaciones y sistemas son iguales y no consideren que utilicen datos muy importantes es necesario saber sobre los tipos y clasificaciones de las vulnerabilidades así como los ejemplos más comunes y su impacto en el sistema, las categorías generales para las vulnerabilidades son las siguientes:

- Critica -- permiten la propagación de amenazas sin ser necesaria la participación del usuario, lo que la convierte en un peligro potencial en un sistema.

- Importante -- puede poner en riesgo los 3 pilares básicos de la seguridad de la información (la confidencialidad, integridad y disponibilidad)

- Moderada -- son sencillas de combatir, su nivel de riesgo puede disminuir con medidas de nivel básico o medio en seguridad, debido a su nivel estas no son aprovechables en todo su potencial y en la mayoría de los casos no logra afectar a los usuarios en

- Baja -- su impacto es mínimo y es muy difícil que un atacante saque provecho de ella.

Algunas de las vulnerabilidades más usadas y conocidas en el mundo informático son las siguientes:

Vulnerabilidades de desbordamiento de buffer

Según TECNOLOGIA-INFORMATICA [Sitio web]. [Consulta: 11 de mayo del 2019] disponible en: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

> "Esta condición se cumple cuando una aplicación no es capaz de controlar la cantidad de datos que se copian en buffer, de forma que si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Este problema se puede aprovechar para ejecutar código que le otorga a un atacante privilegios de administrador." [5]

Vulnerabilidades de condición de carrera (race condition)

Según TECNOLOGIA-INFORMATICA [Sitio web]. [Consulta: 11 de mayo del 2019] disponible en: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

> "La condición de carrera se cumple generalmente cuando varios procesos tienen acceso a un recurso compartido de forma simultánea. En este sentido, un buen ejemplo son las variables, cambiando su estado y obteniendo de esta forma un valor no esperado de la misma." [6]

5, tecnología-informática.com Serie 27000, vulnerabilidades informáticas, 2017

6, tecnología-informática.com Serie 27000, vulnerabilidades informáticas, 2017

Vulnerabilidades de error de formato de cadena (format string bugs)

Según TECNOLOGIA-INFORMATICA [Sitio web]. [Consulta: 11 de mayo del 2019] disponible en: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

> "El motivo fundamental de los llamados errores de cadena de formato es la condición de aceptar sin validar la entrada de datos proporcionada por el usuario. Este es un error de diseño de la aplicación, es decir que proviene de descuidos en su programación. En este sentido el lenguaje de programación más afectado por este tipo de vulnerabilidades es C/C++. Un ataque perpetrado utilizando este método definitivamente conduce a la ejecución de código arbitrario y al robo de información y datos del usuario." [7]

Vulnerabilidades de Cross Site Scripting (XSS)

Según TECNOLOGIA-INFORMATICA [Sitio web]. [Consulta: 11 de mayo del 2019] disponible en: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

> "Las vulnerabilidades del tipo Cross Site Scripting (XSS) son utilizadas en ataques en donde las condiciones permitan ejecutar scripts de lenguajes como VBScript o JavaScript. Es posible encontrar este tipo de situaciones en cualquier aplicación que se utilice para mostrar información en un navegador web cualquiera, que no se encuentre debidamente protegido contra estos ataques." [8]

7, tecnología-informática.com Serie 27000, vulnerabilidades informáticas, 2017

8, tecnología-informática.com Serie 27000, vulnerabilidades informáticas, 2017

Vulnerabilidades de Inyección SQL

Según TECNOLOGIA-INFORMATICA [Sitio web]. [Consulta: 11 de mayo del 2019] disponible en: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

> "Las llamadas "vulnerabilidades de inyección SQL" se producen cuando mediante alguna técnica se inserta o adjunta código SQL que no formaba parte de un código SQL programado. Esta técnica se utiliza con el propósito de alterar el buen funcionamiento de la base de datos de una aplicación, "inyectando" código foráneo que permita el proceso de datos que el atacante desee." [9]

Vulnerabilidades de denegación del servicio

Según TECNOLOGIA-INFORMATICA [Sitio web]. [Consulta: 11 de mayo del 2019] disponible en: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

> "La técnica de denegación de servicio se utiliza con el propósito de que los usuarios no puedan utilizar un servicio, aplicación o recurso. Básicamente lo que produce un ataque de denegación de servicio es la pérdida de la conectividad de la red de la víctima del ataque por el excesivo consumo del ancho de banda de la red o de los recursos conectados al sistema informático." [10]

Vulnerabilidades de ventanas engañosas

Según TECNOLOGIA-INFORMATICA [Sitio web]. [Consulta: 11 de mayo del 2019] disponible en: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

> "Sin duda esta es una de las vulnerabilidades más conocidas y comunes entre los usuarios, sobre todo para aquellos que ya llevan algunos años tras un monitor. Esta técnica, también conocida como "Window Spoofing" permite que un atacante muestre ventanas y mensajes de notificación en la computadora de la víctima, que generalmente consisten en hacernos saber que somos ganadores de un premio o situaciones similares." [11]

9, tecnología-informática.com Serie 27000, vulnerabilidades informáticas, 2017

10, tecnología-informática.com Serie 27000, vulnerabilidades informáticas, 2017

11, tecnología-informática.com Serie 27000, vulnerabilidades informáticas, 2017

7.3 HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES

Las herramientas de análisis de vulnerabilidades, es software diseñado para analizar un sistema mediante simulación de ataques, exploración de sus características o posibles vulnerabilidades para recopilar toda la información posible sobre las falencias del sistema analizado, esto le permite a un administrador o líder de proceso informático conocer el estado a nivel de seguridad de su sistema y tomar acciones preventivas y correctivas.

Estos software se encuentran distribuidos en diferentes categorías y según el sistema hardware o software que sea objeto del análisis así mismo existe una herramienta especialmente diseñada para esa tarea, para esta monografía hablaremos de dos herramientas en especial NMAP y OPENVAS, existen muchas más claro esta como la bien conocida NESSUS, pero algunas de estas herramientas o bien son de pago y para ejecutar el 100% de sus funciones se necesita realizar dicho pago, otras simplemente están diseñadas para analizar aplicaciones web u otro tipo de sistemas o componentes informáticos, estas herramientas se eligieron debido a su reconocimiento, su comunidad y documentación que brindan a este tipo de procesos respaldo suficiente para realizarlo de la mejor manera posible.

7.4 KALI LINUX

Kali Linux será una de las principales herramientas que se usaran en la actividad de análisis de vulnerabilidades en el servidor central de la E.S.E. Hospital Marco Felipe Afanador de Tocaima, esta distribución de Linux basada en Debían, incluye diferentes herramientas de penetración y auditoría de seguridad muchas de estas son de código abierto para la realización de pruebas de seguridad, Kali Linux fue desarrollado por Offensive Security, su nombre es bien reconocido y confiable en el mundo de la seguridad informática, ya que a su vez es un ente certificador con varias de las certificaciones más respetadas disponibles.

Esta herramienta es muy flexible a la hora de realizar procesos de análisis de vulnerabilidades, pruebas de penetración y demás relacionadas con la seguridad informática al ser una solución portable que no requiere una instalación es prácticamente la navaja suiza de un informático que se enfoque a la seguridad informática.

7.5 NMAP Y OPENVAS

OpenVas es una herramienta de escaneo y análisis de vulnerabilidades opensource con la capacidad de realizar informes de las vulnerabilidades detectadas en el sistema analizado, así como proporcionar la información sobre las posibles soluciones, esta herramienta ofrece a sus usuarios una interfaz gráfica GUI, amigable acompañado de guías y una comunidad que ofrece documentación teórico practica de todas las opciones y accione que se pueden realizar con esta herramienta

Dentro de las principales características de esta herramienta encontramos:

- Puede realizar escaneo de forma simultánea en varios equipos
- Soporta el protocolo SSL
- Se pueden programas los escaneos
- Ofrece versatilidad administrativa permitiendo detener un análisis si es necesario
- Se puede administrar desde consola
- Soporta HTTP y HTTPS
- Soporta multilenguaje
- Es Multiplataforma
- Sus Reportes son claros y completos
- Es gratuito

Nmap es una herramienta que se utiliza para el escaneo y análisis de redes en las permitiendo explorar, administrar y auditar la seguridad de redes, esta herramienta Detecta hosts que estén en línea analizando, sus puertos abiertos, servicios y aplicaciones que corren en ellos, adicionalmente también podemos recopilar información adicional como su sistema operativo, firewalls y sus filtros entre otro tipo de información que sería relevante para un atacante, este software es una excelente opción para hacer trabajos de auditoria debido a que fue diseñado para realizar escaneos rápidos y precisos en una gran cantidad de redes, los 3 usos más frecuentes para esta herramienta son:

- Auditorias de seguridad informática.
- Pruebas rutinarias de redes.
- Recolector de información para futuros ataques

AL igual que OPENVAS, NMAP es un software libre y por lo tanto gratuito, y otra similitud que comparte es que son multiplataforma existiendo una versión para cada sistema operativo (MacOSX, Microsoft Windows, GNU/Linux, OpenBSD, Solaris, etc.)

8. PRESENTACIÓN DE LAS HERRAMIENTAS QUE SE VAN A UTILIZAR

Para iniciar el análisis de vulnerabilidades trabajaremos con 4 herramientas, que serán Virtual Box, “figura1”, Kali Linux “figura 2”, Nmap y OpenVas “figuras 3 y 4 respectivamente”, a continuación se presentar las herramientas que vamos a utilizar para este proceso, describiendo su función, esto no será tan a fondo pero si las partes más relevantes de estas, ya que ese no es el fin de este análisis, nos enfocaremos en los procesos que nos ayudaran a descubrir las vulnerabilidades del servidor

8.1 VIRTUAL BOX

Figura 1 Virtual Box Logo

Fuente: Google: Virtual Box Logo

Virtual Box es un software de virtualización que permite emular diferentes tipos de sistemas operativos desde Windows, Linux, Mac, pasando por sistemas operativos alternativos como Remix OS, en este software emularemos nuestra herramienta principal para el análisis que será Kali Linux.

8.2 KALI LINUX

Figura 2 Kali Linux Logo

Fuente: Google: Kali Linux Logo

Kali Linux será una de las principales herramientas que se usaran en la actividad de análisis de vulnerabilidades en el servidor central de la E.S.E. Hospital Marco Felipe Afanador de Tocaima, esta distribución de Linux basada en Debían, incluye diferentes herramientas de penetración y auditoría de seguridad muchas de estas son de código abierto para la realización de pruebas de seguridad, Kali Linux fue desarrollado por Offensive Security, su nombre es bien reconocido y confiable en el mundo de la seguridad informática, ya que a su vez es un ente certificador con varias de las certificaciones más respetadas disponibles.

Esta herramienta es muy flexible a la hora de realizar procesos de análisis de vulnerabilidades, pruebas de penetración y demás relacionadas con la seguridad informática al ser una solución portable que no requiere una instalación es prácticamente la navaja suiza de un informático que se enfoque a la seguridad informática

8. 3 NMAP

Figura 3 Nmap Logo

Fuente: Google Nmap Logo

Openvas es una herramienta de escaneo y análisis de vulnerabilidades opensource con la capacidad de realizar informes de las vulnerabilidades detectadas en el sistema analizado, así como proporcionar la información sobre las posibles soluciones, esta herramienta ofrece a sus usuarios una interfaz gráfica GUI, amigable acompañado de guías y una comunidad que ofrece documentación teórico practica de todas las opciones y accione que se pueden realizar con esta herramienta

Dentro de las principales características de esta herramienta encontramos:

- Puede realizar escaneo de forma simultánea en varios equipos
- Soporta el protocolo SSL
- Se pueden programas los escaneos
- Ofrece versatilidad administrativa permitiendo detener un análisis si es necesario
- Se puede administrar desde consola
- Soporta HTTP y HTTPS
- Soporta multilenguaje
- Es Multiplataforma
- Sus Reportes son claros y completos
- Es gratuito

Nmap es una herramienta que se utiliza para el escaneo y análisis de redes en las permitiendo explorar, administrar y auditar la seguridad de redes, esta herramienta Detecta hosts que estén en línea analizando, sus puertos abiertos, servicios y aplicaciones que corren en ellos, adicionalmente también podemos recopilar información adicional como su

sistema operativo, firewalls y sus filtros entre otro tipo de información que sería relevante para un atacante, este software es una excelente opción para hacer trabajos de auditoria debido a que fue diseñado para realizar escaneos rápidos y precisos en una gran cantidad de redes, los 3 usos más frecuentes para esta herramienta son:

- Auditorias de seguridad informática.
- Pruebas rutinarias de redes.
- Recolector de información para futuros ataques

8.4 OPENVAS

Figura 4 OpenVas Logo

Fuente: Google OpenVas logo

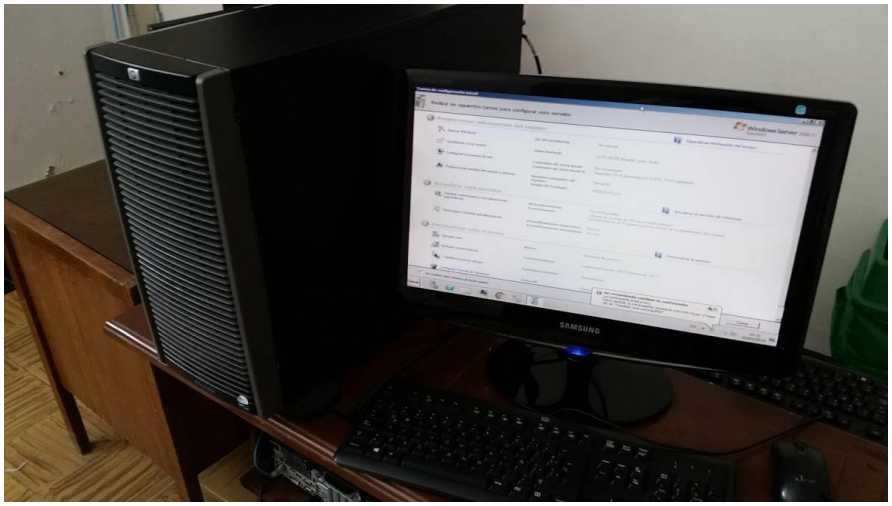
OpenVas será la herramienta clave para este análisis; Es un escáner de vulnerabilidades de libre uso o licencia gratuita para la identificación posibles vulnerabilidades informáticas en los host de una red, este framework “esquema de trabajo, herramientas y servicios predefinidos estructuralmente” cuenta con diferentes servicios y herramientas base para evaluar vulnerabilidades convirtiéndolo en una herramienta versátil que se puede usar en conjunto con otras herramientas que realizan otros tipos de análisis.

Su potencias y características permiten generar un informe detallado de las vulnerabilidades detectadas permitiendo a un administrador de red o profesional de auditoria detectar el tipo de vulnerabilidad y corregirla gracias a la información que openvas de proporciona

9. ANÁLISIS DE VULNERABILIDADES

Se procede a realizar el primer análisis de vulnerabilidades en el servidor de pruebas de la E.S.E. Hospital Marco Felipe Afanador de Tocaima “figura 5”, este es realizado un fin de semana para evitar inconvenientes a nivel de producción.

Figura 5 Servidor de pruebas E.S.E. Hospital Marco Felipe Afanador de Tocaima



Fuente: Elaboración Propia

9.1 VIRTUAL BOX

El único fin de este software en este análisis de vulnerabilidades es virtualizar nuestro sistema operativo Kali Linux y así evitar instalaciones innecesarias o las cuales no se tiene permiso de ejecutar, en las figura 6 se observa la página oficial de descarga y en las figuras 7, 8 y 9 verán algunas ventanas de la configuración de este software

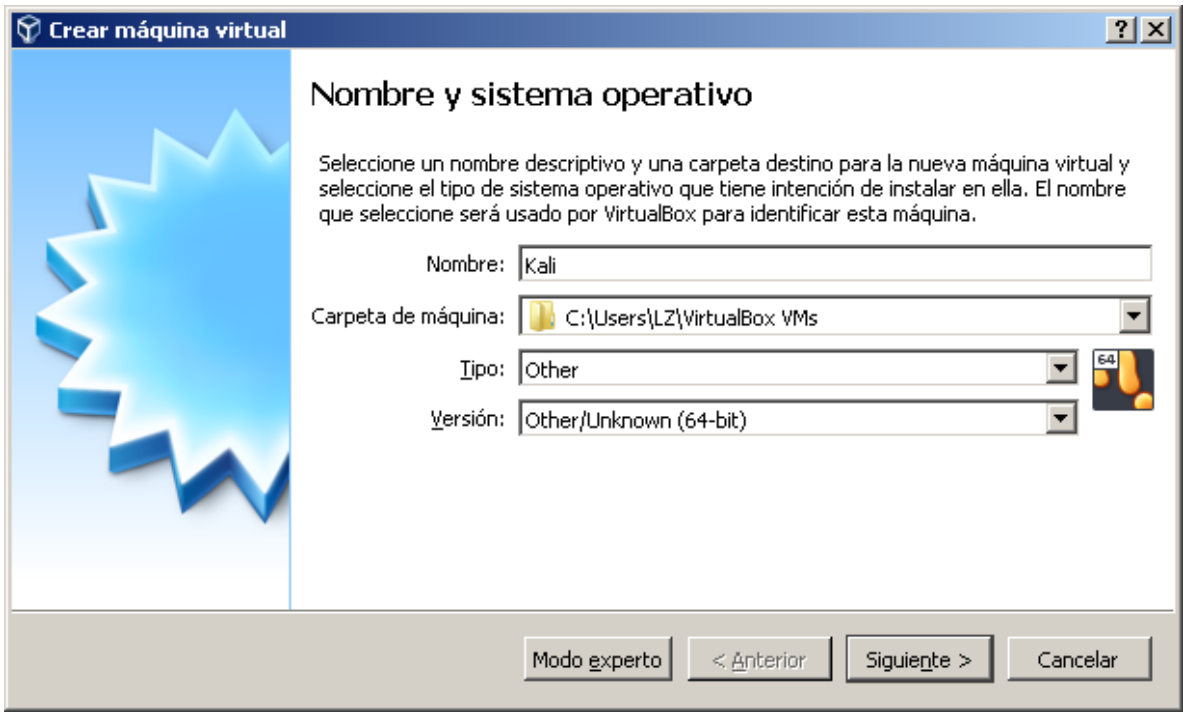
Figura 6 Página Oficial de Virtual Box

Fuente: www.virtualbox.org

Figura 7 Interfaz de Virtual Box

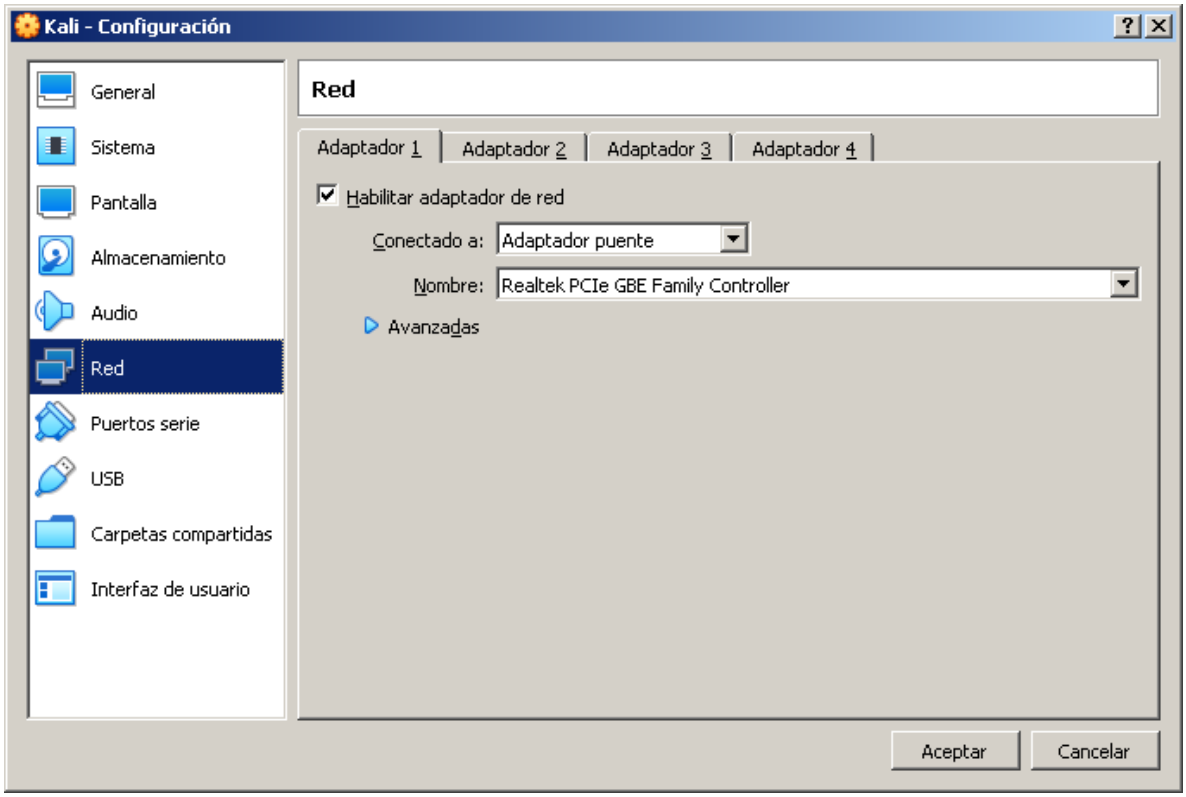
Fuente: Elaboración Propia

Figura 8 Creación de Máquina Virtual Kali Linux



Fuente: Elaboración Propia

Figura 9 Configuración de red Virtual Box



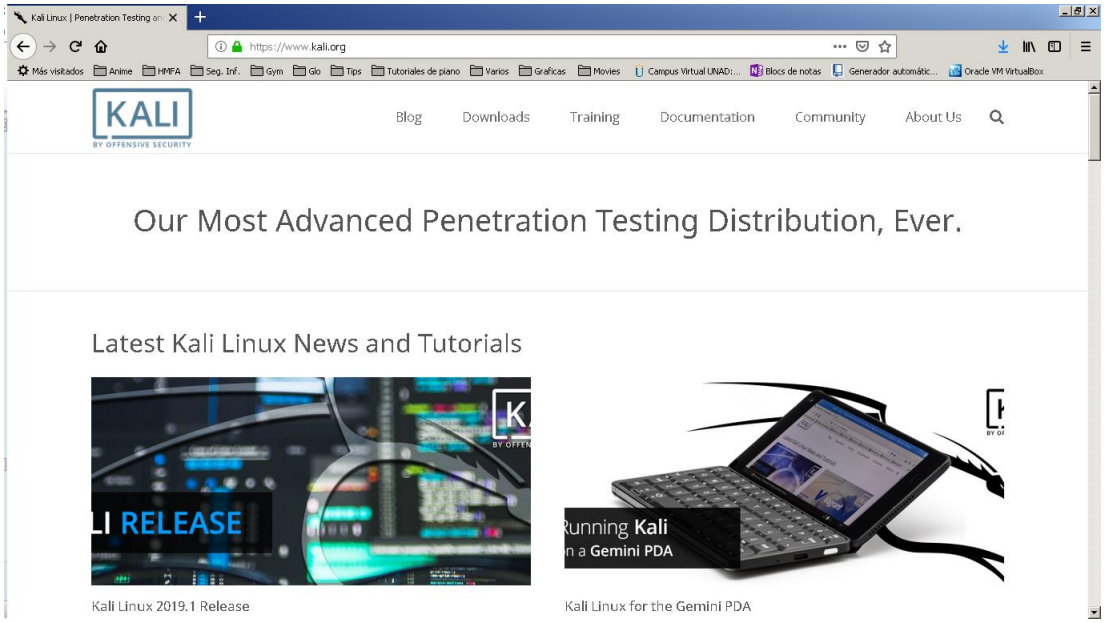
Fuente: Elaboración Propia

9.2 KALI LINUX

Esta será la herramienta base que se usara en el análisis de vulnerabilidades, debido a que trae integrados los software que vamos a usar, “ Nmap y Openvas” lo que facilita el desarrollo de la actividad, como consejo adicional y para evitar posibles fallos en este tipo de pruebas se recomienda siempre utilizar la última versión disponible en la página oficial y a menos de que se tenga un muy buen nivel en este tipo de herramientas, es recomendable descargar la versión para Virtual Box debido a que esta versión se desenvuelve de una forma mucho más óptima que emulando la imagen ISO de este sistema operativo.

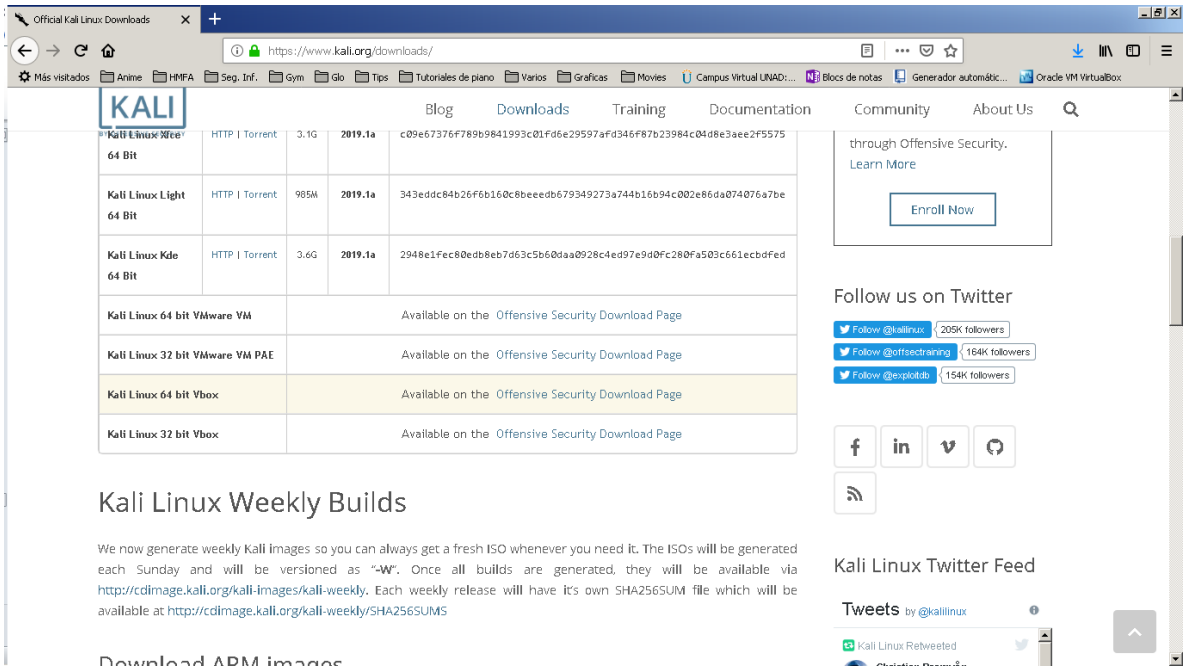
En las figuras 10 y 11 se observa la página oficial y la descarga de la imagen recomendada a utilizar para este tipo de operación, en las figuras 12, 13 ,14 y 15, se veran varias imágenes de la interfaz de Kali Linux

Figura 10 Página Oficial de Kali Linux



Fuente: www.kali.org

Figura 11 Kali Linux descarga de imagen recomendada



Fuente: www.Kali.org/downloads

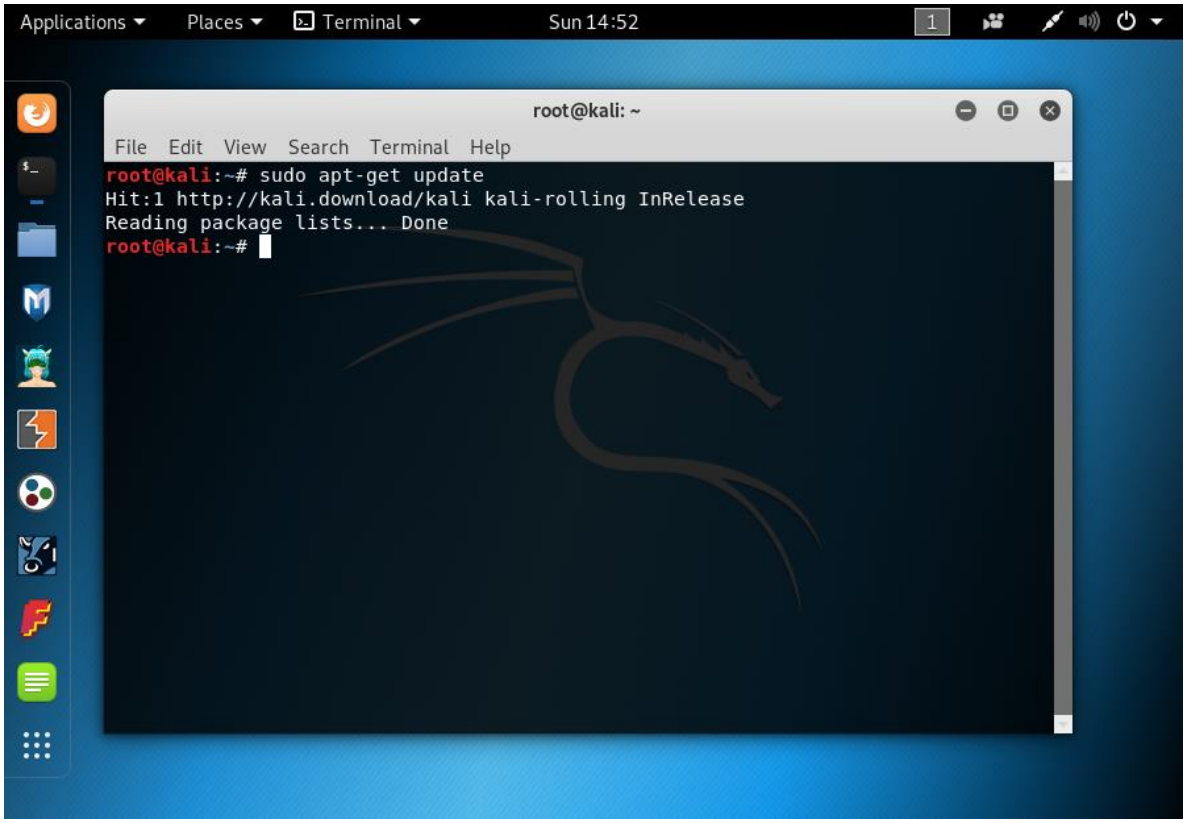
Figura 12 Ejecución de Kali Linux en Virtual Box

Fuente: Elaboración Propia

Figura 13 Escritorio de Kali Linux

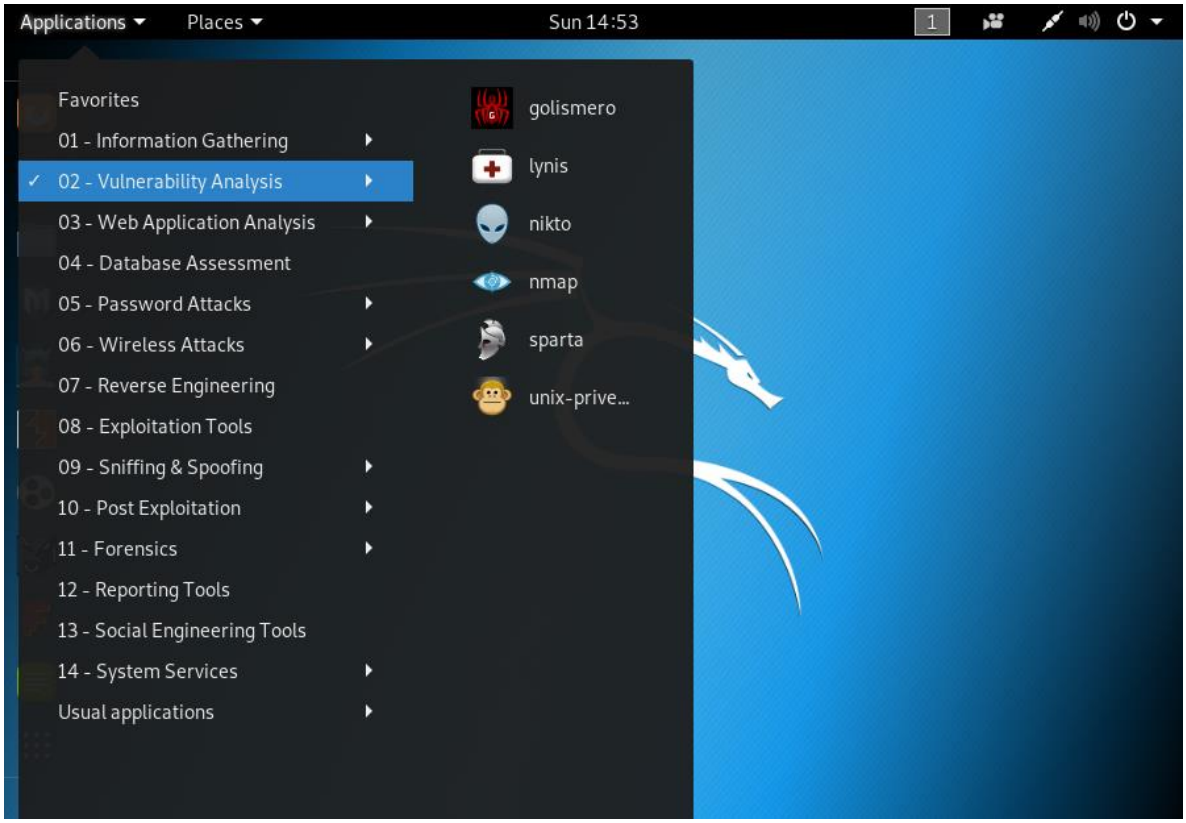
Fuente: Elaboración Propia

Figura 14 Actualización de los paquetes de Kali Linux por línea de comandos



Fuente: Elaboración Propia

Figura 15 Menú de herramientas de análisis de vulnerabilidades Kali Linux

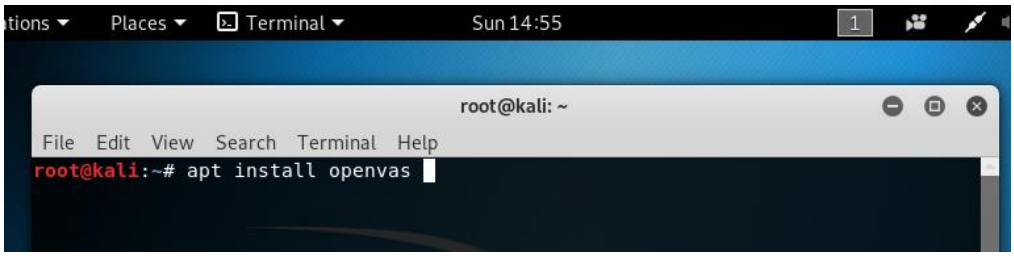


Fuente: Elaboración Propia

9.2.1 Instalación de OpenVas. En algunas ocasiones y según la versión con la que se trabaje de Kali Linux existe la posibilidad de que no se encuentre instalada la herramienta OpenVas en este sistema operativo, en tal caso lo que se debe hacer es lo siguiente:

1. Abrir la consola de comandos "figura 16" y digitar **apt install** openvas, en otros casos hay que digitar sudo **apt-get install** open vas ambas opciones son válidas pero en ocasiones hay que hacer uso de la segunda línea de comandos.

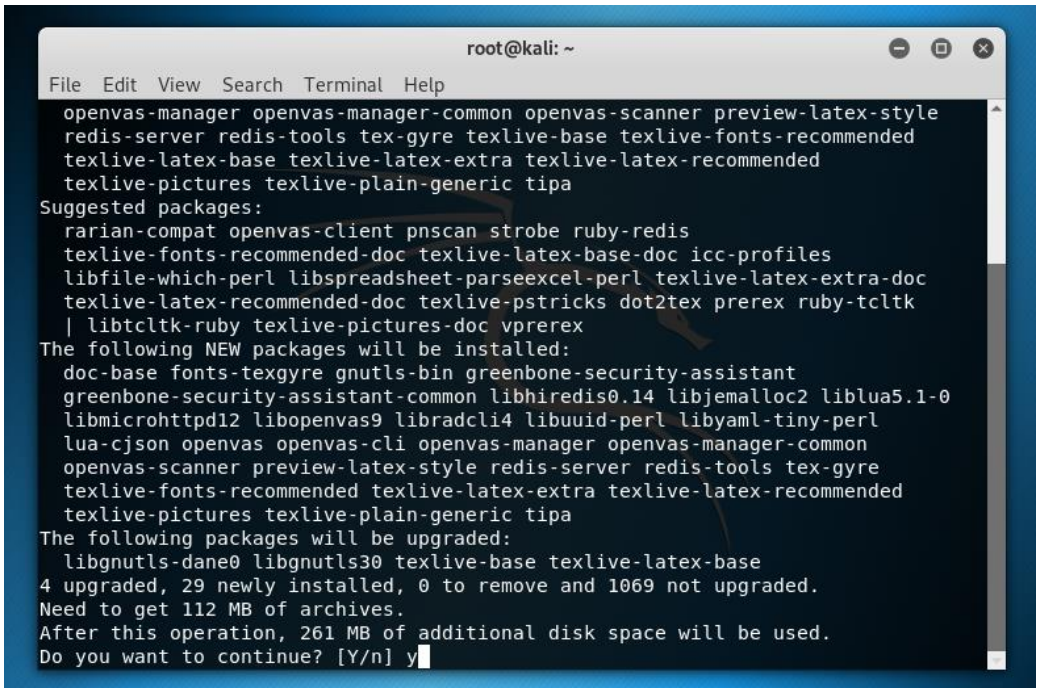
Figura 16 Instalación de OpenVas – 1



Fuente: Elaboración Propia

2. Después de digitar alguna de las dos opciones se debe esperar hasta que nos aparezcan varias líneas de comandos "figura 17" que muestran el progreso de la instalación, nos preguntaran si se desea continuar y se debe escribir **Y**

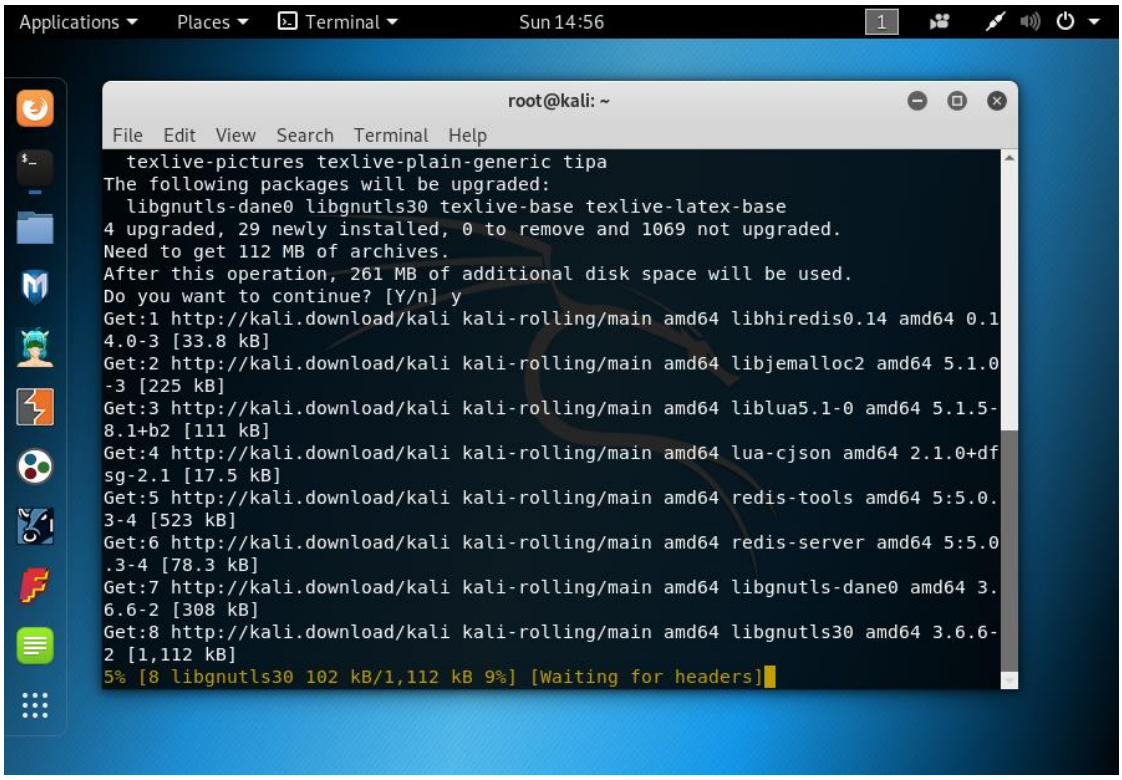
Figura 17 Instalación de OpenVas – 2



Fuente: Elaboración Propia

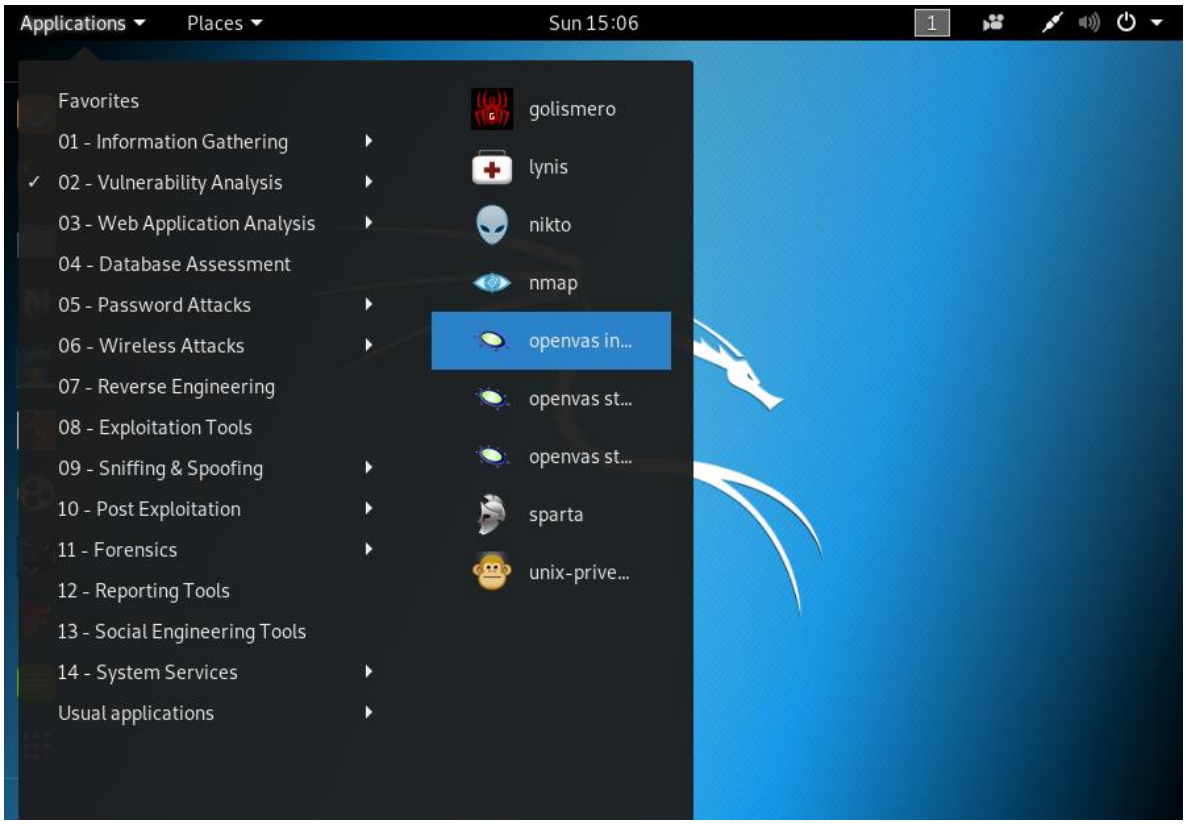
3. Ya por ultimo solo resta esperar la instalación “figura 18” y luego se debe buscar el programa en el menú de kali Linux “figura 19” en el apartado de programas para análisis de vulnerabilidades

Figura 18 Instalación de OpenVas – 3



Fuente: Elaboración Propia

Figura 19 OpenVas en el menú de análisis de vulnerabilidades kali Linux

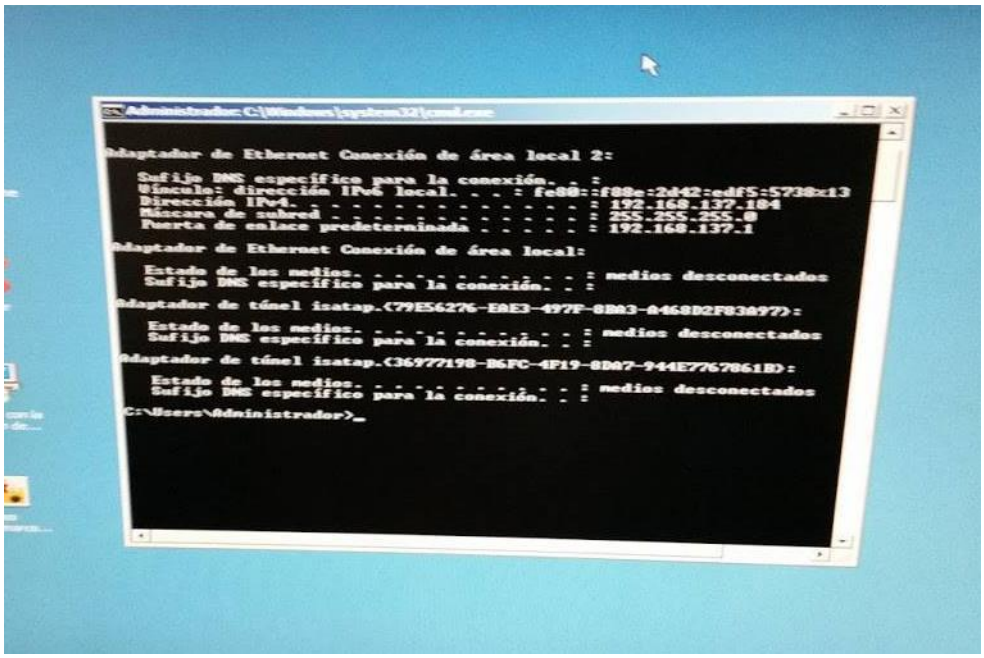


Fuente: Elaboración Propia

9.3 RED Y CONECTIVIDAD

Antes de iniciar el proceso de análisis de vulnerabilidades, hay que comprobar que existe conectividad entre el equipo anfitrión “figura 20” donde se tiene virtualizado Kali Linux y el servidor, el servidor de pruebas tiene el direccionamiento 192.168.137.184, así que se hará una prueba de conexión “figura 21” mediante un ping desde el kali Linux

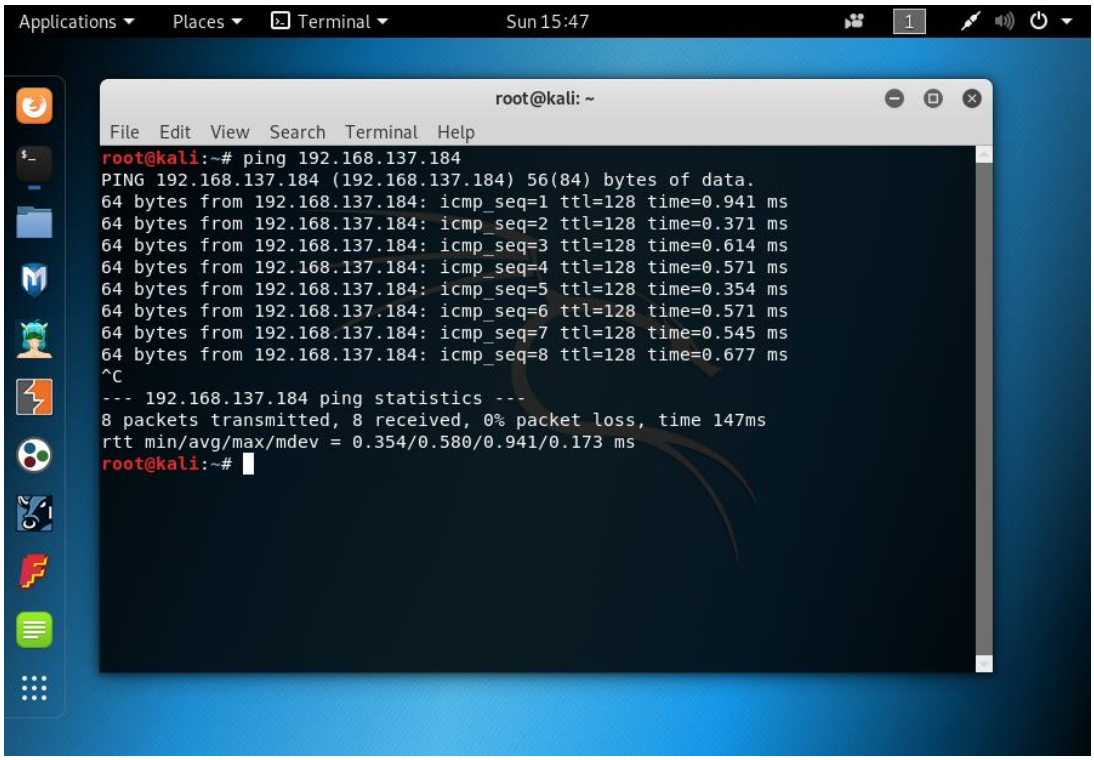
Figura 20 Dirección Ip Servidor de Pruebas



Fuente: Elaboración Propia

Al realizar un ping hacia esa dirección IP se observa que el resultado es positivo y existe conectividad entre la máquina y el servidor

Figura 21 Prueba de Ping desde la máquina Virtual



Fuente: Elaboración Propia

9.4 ANÁLISIS CON NMAP

Ahora se usara Nmap para descubrir información de posibles vulnerabilidades de a nivel de Red

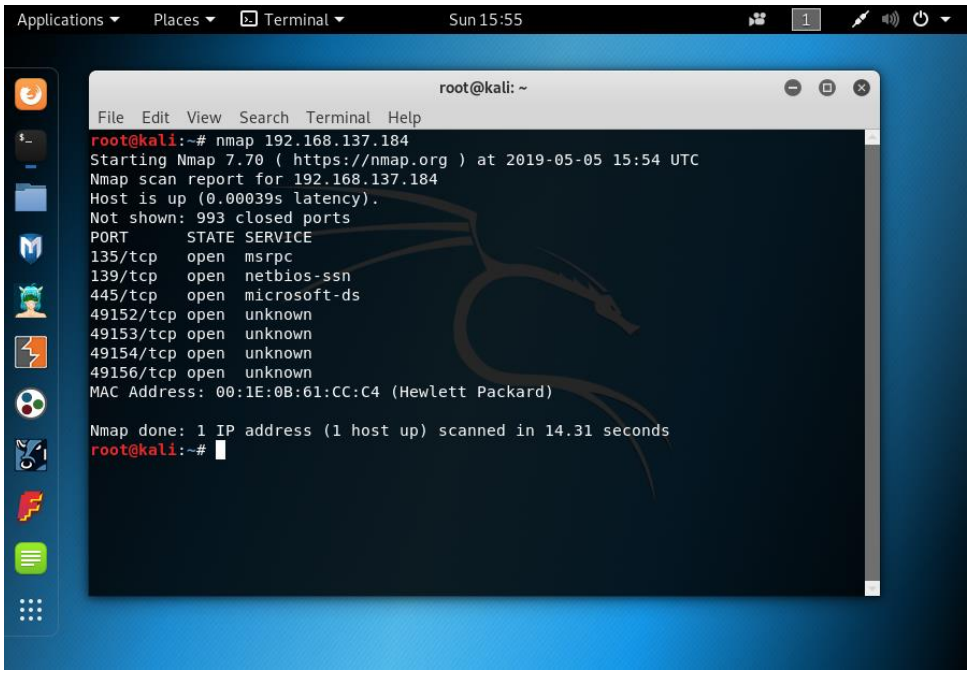
9.4.1 COMANDOS A UTILIZAR

Para esta fase se usaran los siguientes comandos:

- Nmap -sV
- Nmap -A
- Nmap + IP del objetivo

9.4.1.1 Nmap + Ip del Host. Este es uno de los análisis más básicos que se pueden ejecutar en Nmap, al realizar este comando solo se observan los puertos cerrados los puertos su estado y el servicio que se está ejecutando de una manera básica “figura 22", si dirección MAC y la marca del equipo.

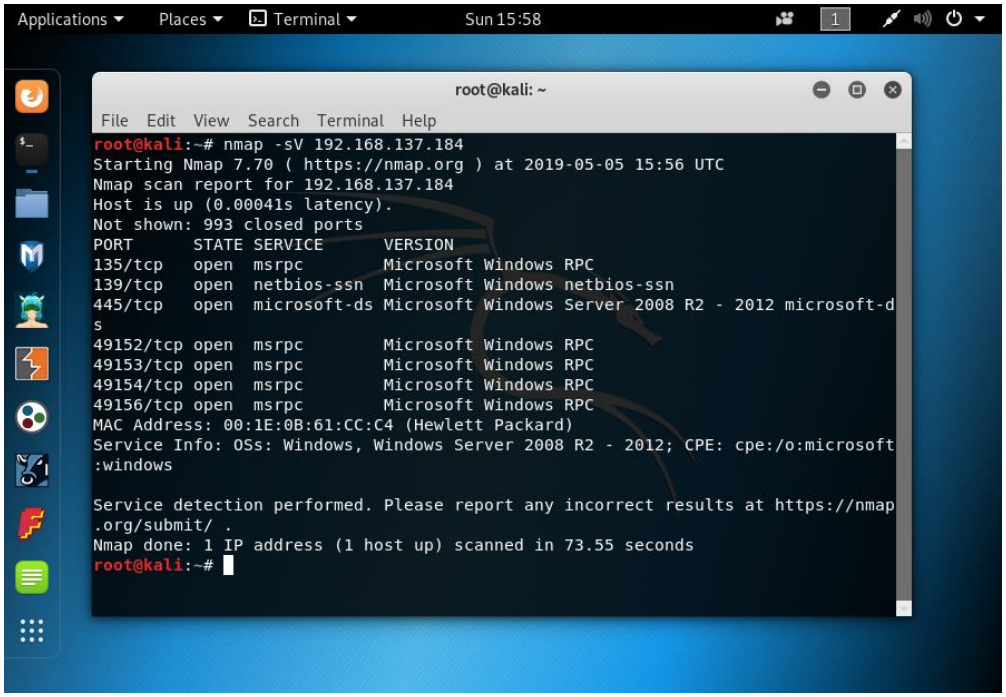
Figura 22 Nmap + Ip del Host



Fuente: Elaboración Propia

9.4.1.2 Nmap – Sv. Este comando “figura 23” permite ver los puertos del host que se está escaneando, su estado que por lo general es abierto, el tipo de servicio que se está ejecutando por ese puerto y su versión, adicional a eso se observa a manera de resumen los puertos que están cerrados que en esta caso son 993 puertos, se observa también la versión del sistema operativo que es un Windows Server 2008 R2 y su dirección Mac

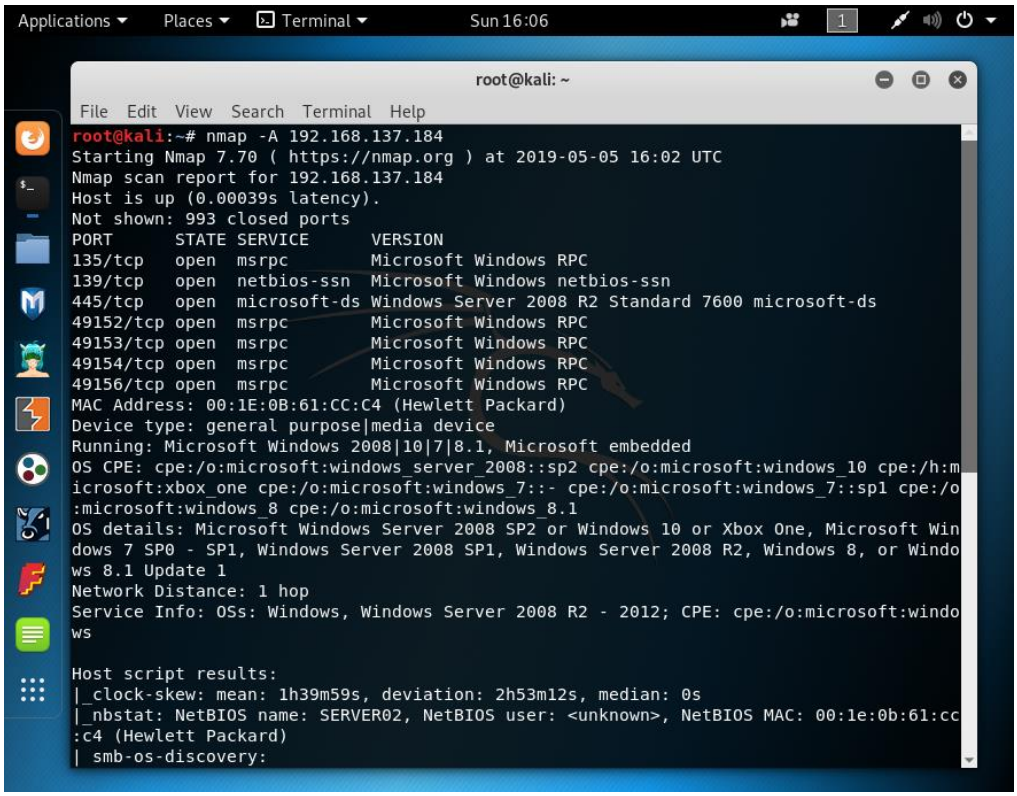
Figura 23 Nmap –sV



Fuente: Elaboración Propia

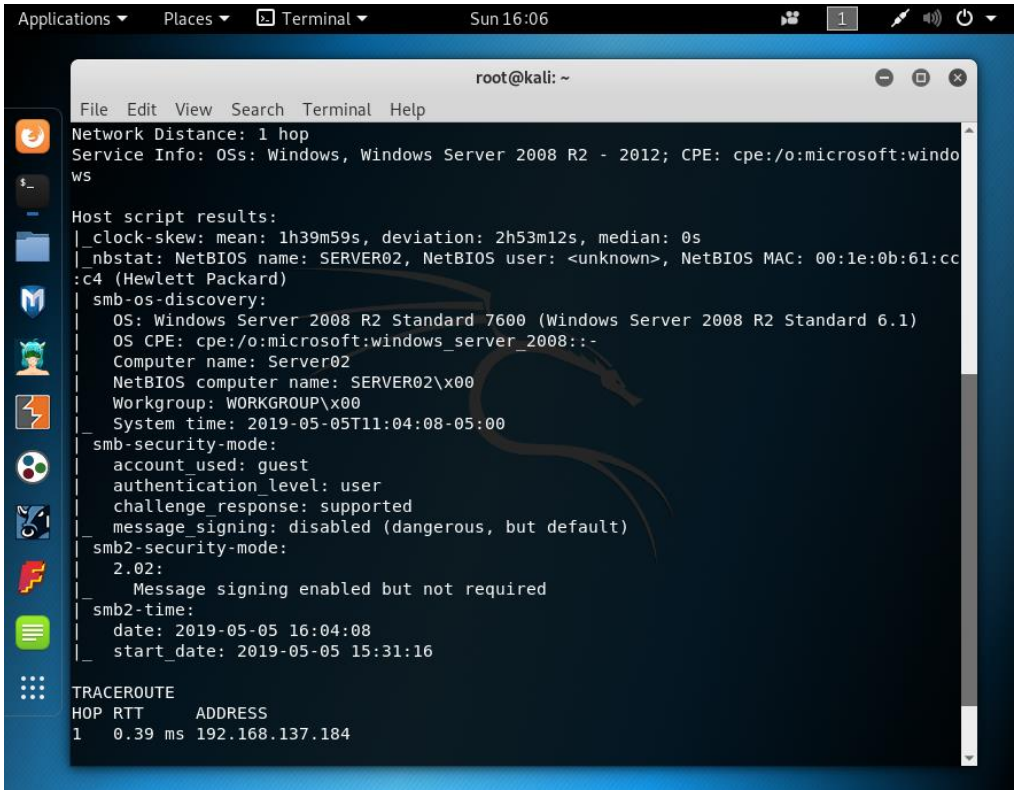
9.4.1.3 Nmap – A. Este comando “figura 24” es una versión del –Sv pero mucho mejor, ya que le añade un traceroute “opción que nos permite ver los saltos o host que hay antes de llegar a nuestro equipo objetivo” adicionado información adicional gracias a sus Script por default, “figura 25” cuando se usa este comando podemos observar a parte de los puertos que se ven con el –Sv, la marca del equipo en este caso HP (Hewlett Packard), el sistema operativo que se está ejecutando y su versión 6.1, los saldos o host que hay entre el equipo anfitrión y el servidor que en este caso es solo 1, se observa el nombre del equipo, el grupo de trabajo, la hora del equipo y ya empezamos a observar datos como la seguridad en su SMB “Server Menssage Blocks” que es el protocolo de red que permite compartir archivos impresoras y demás recursos en red.

Figura 23 Nmap -A -- parte 1



Fuente: Elaboración Propia

Figura 24 Nmap -A -- Parte 2

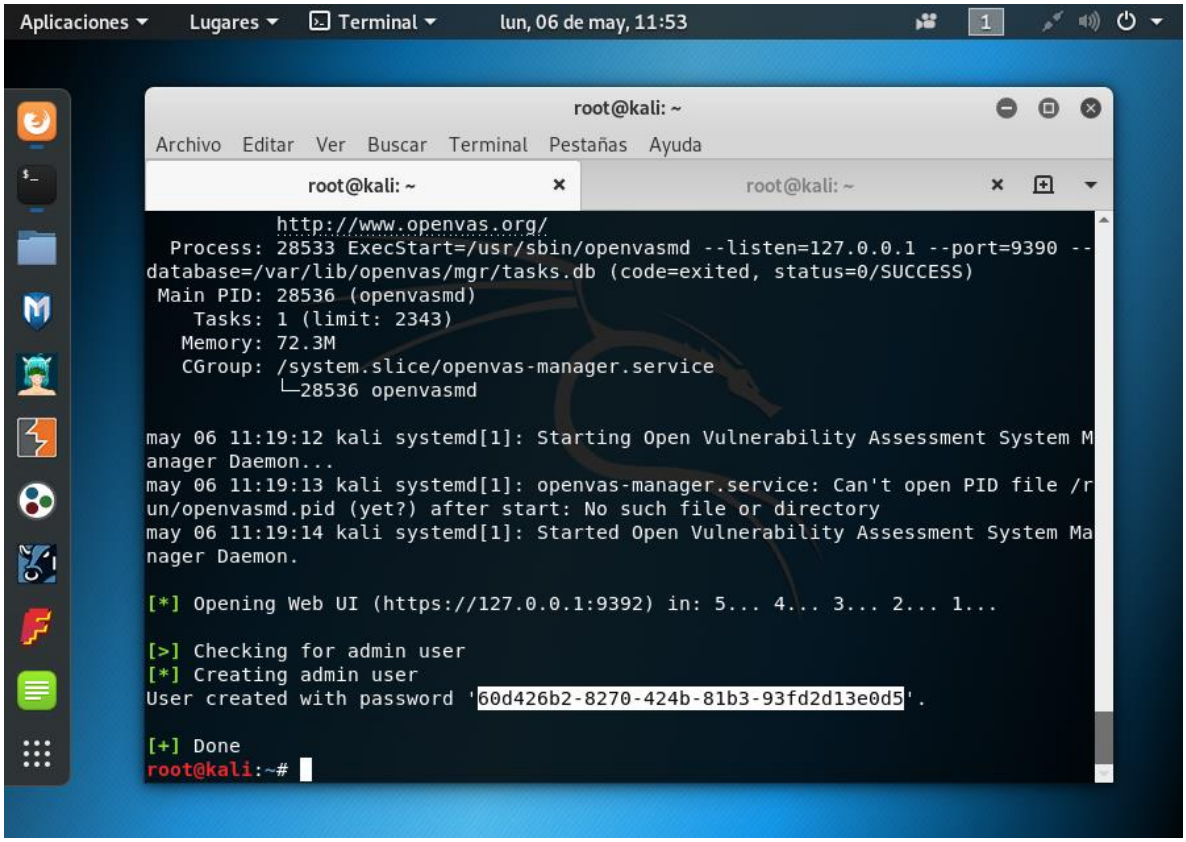


Fuente: Elaboración Propia

9.5 Análisis con OpenVas

Ahora pasamos a ejecutar el análisis con la herramienta de detección de vulnerabilidades OpenVas, “figura 26” como se estipula en el numeral 8 de esta monografía, no se profundizara en todos los pasos de la instalación debido a que ese no es el objetivo, pero de igual forma se plasmaran los pasos cruciales en el proceso con esta herramienta

Figura 25 Análisis con OpenVas 1

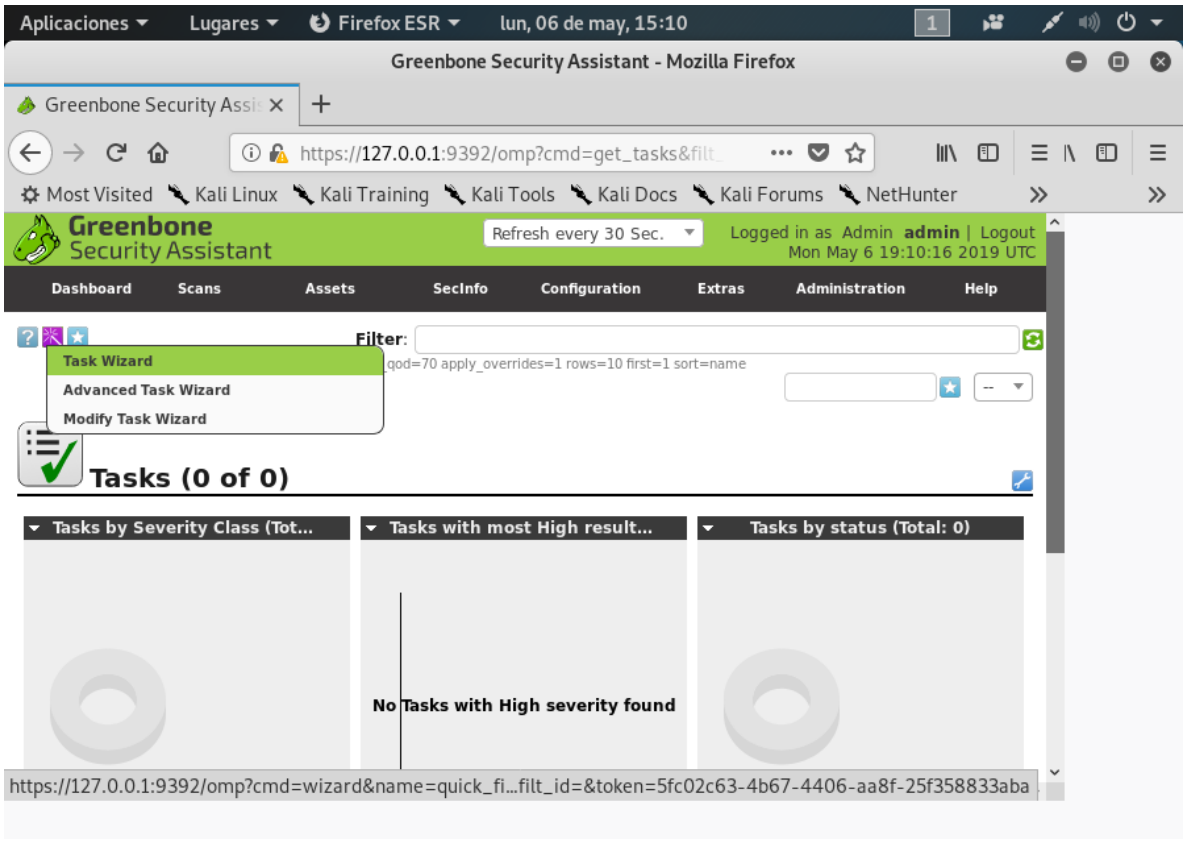


Fuente: Elaboración Propia

Cuando se inicia el programa de OpenVas este proporciona el usuario y la contraseña para ingresar al entorno administrativo del software.

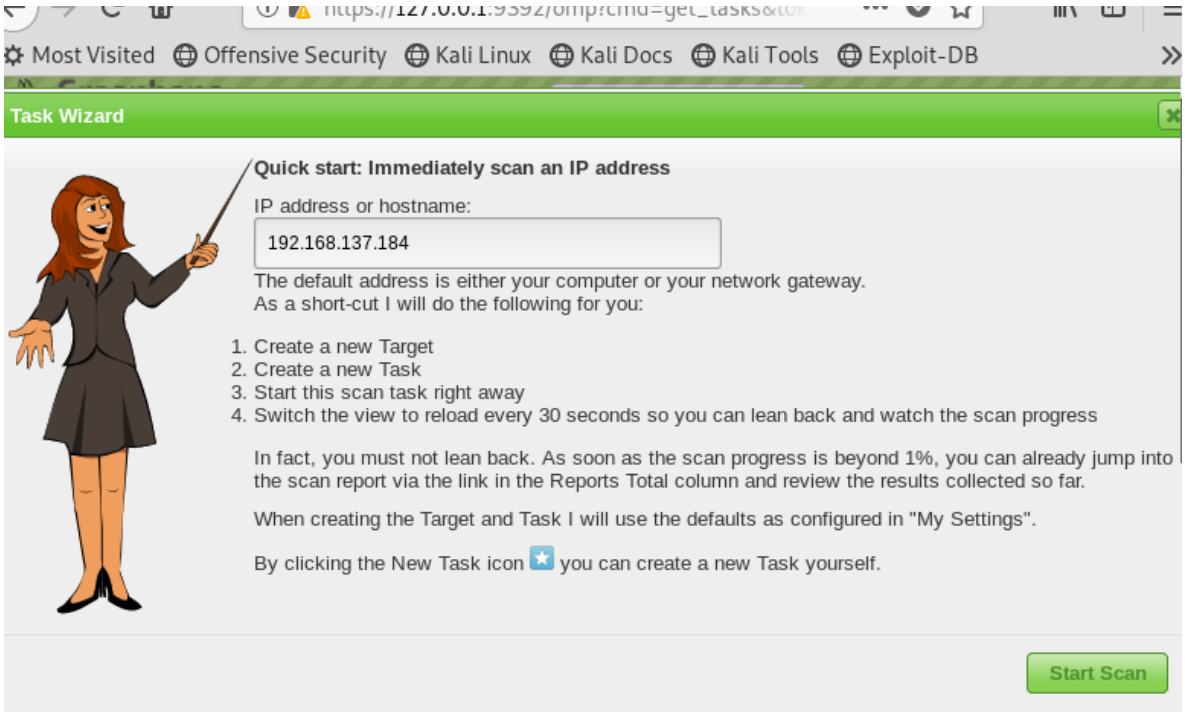
Una vez se ingresa al entorno administrativo denominado Greenbone “figura 27 y 28”, se procede a crear la terea para realizar el análisis, en openvas existen dos maneras de realizar el análisis por medio de wizard o por medio de la tarea avanzada, esta última está dedicada a usuarios más experimentados que requieran hacer configuraciones especiales al análisis, como se realizara un análisis sencillo se usara el wizard para esta tarea.

Figura 26 Análisis con OpenVas 2 - interfaz principal



Fuente: Elaboración Propia

Figura 27 OpenVas Wizard

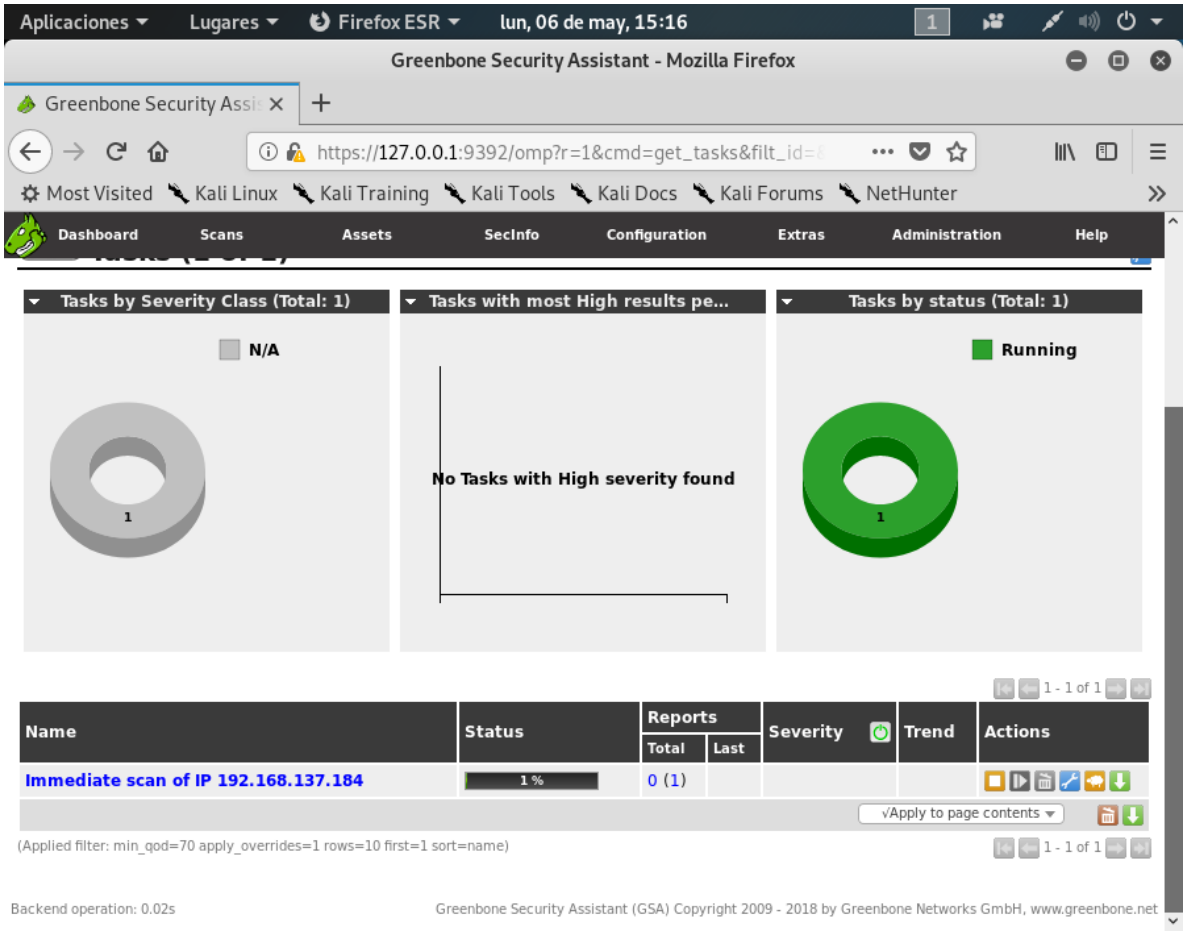


Fuente: Elaboración Propia

El wizard es ideal para principiantes que deseen explorar las herramientas sin ninguna configuración adicional, o si el escaneo de las vulnerabilidades no requiere de configuraciones avanzadas en este paso solo se coloca la dirección IP del host objetivo para el análisis y el programa se encargara del resto, solo queda esperar el resultado de las vulnerabilidades encontradas.

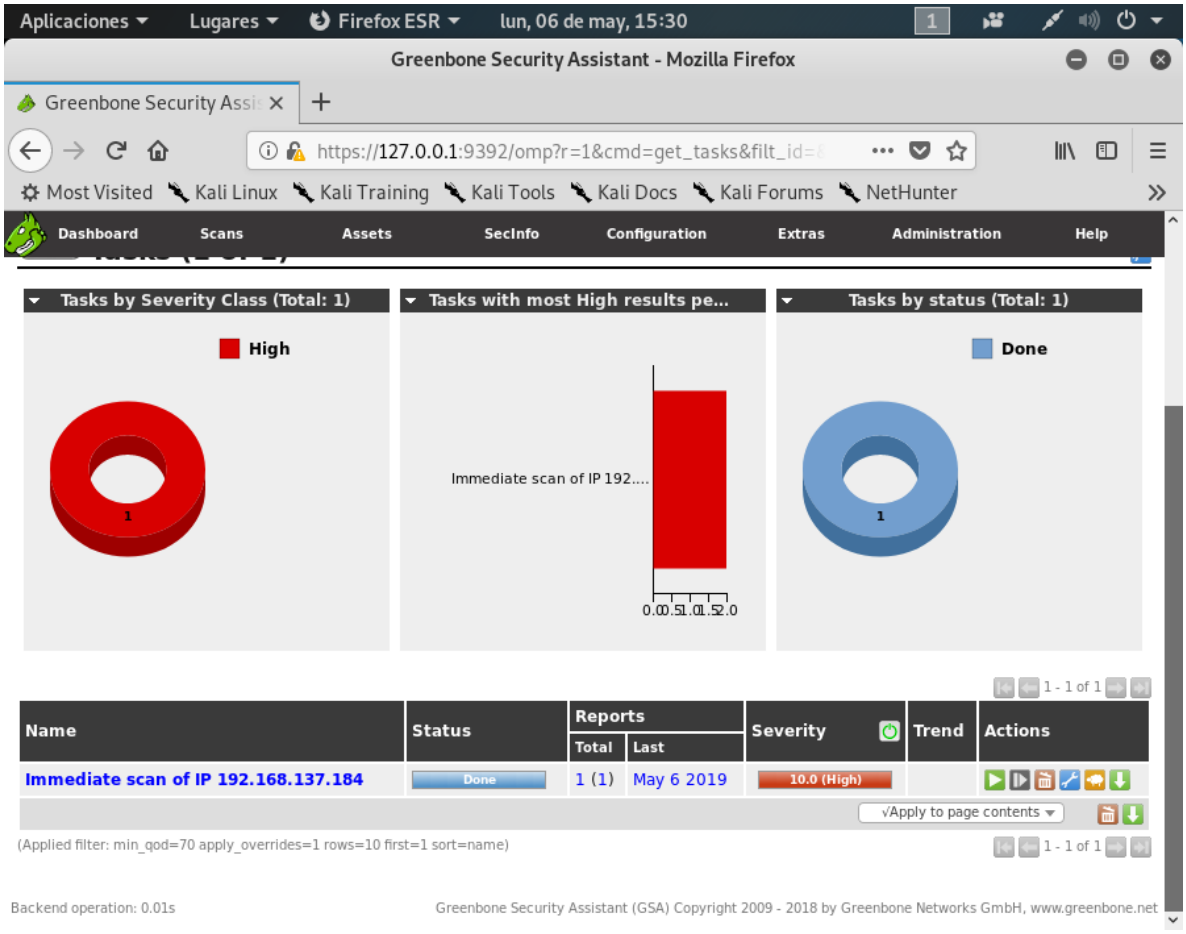
Acá se puede observar cómo se ejecuta el análisis de vulnerabilidades en la interfaz Greenbone de openvas, “figura 29 y 30” el porcentaje de progreso y avance de este proceso varía según el host que se esté analizando así como la cantidad de servicios y vulnerabilidades relacionadas que este pueda presentar.

Figura 28 Inicio Análisis Openvas



Fuente: Elaboración Propia

Figura 29 Análisis Terminado Openvas



Fuente: Elaboración Propia

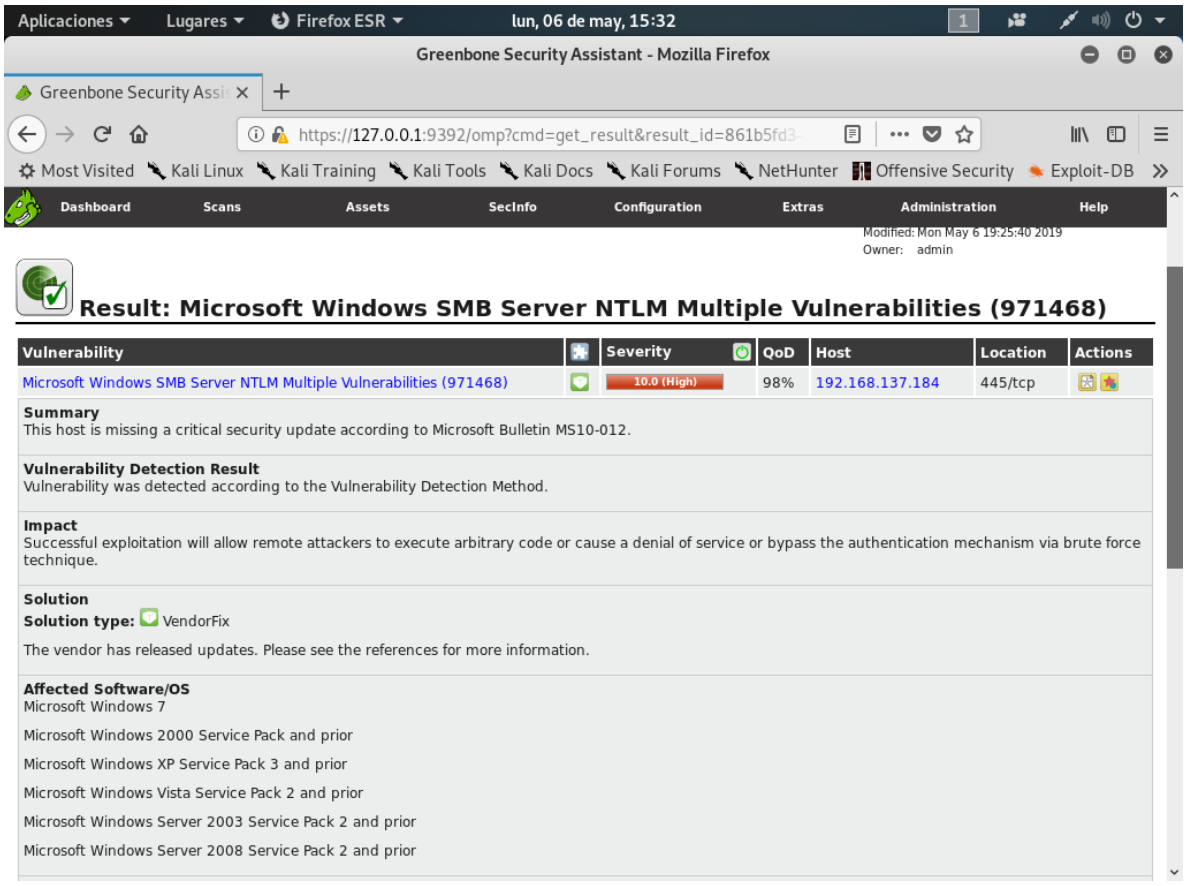
Ahora se puede observar el análisis terminado al 100% cuando este análisis termina solo resta dar doble clic para ver los resultados encontrados.

Los resultados arrojan 3 vulnerabilidades “figura 31 y 32” en el host analizado 2 de tipo alto y una de tipo medio, al dar clic en cualquiera de ellas Greenbone desplegara más información para poder investigar a fondo esta vulnerabilidad y así poder generar las recomendaciones necesarias para el proceso de hardening

Figura 30Vulnerabilidades Encontradas

Fuente: Elaboración Propia

Figura 31 Ejemplo detallado de vulnerabilidad Greenbone



Fuente: Elaboración Propia

10. ANÁLISIS DE RESULTADOS Y RECOMENDACIONES PARA EL PROCESO DE HARDENING

Ahora se procede a analizar los resultados obtenidos en las dos pruebas realizadas, (Nmap y OpenVas:

10.1 RESULTADOS NMAP

Con Nmap se observó un buen nivel de seguridad esto se debe a que el programa detecta 993 puertos cerrados y solo 7 abiertos cada uno con un servicio designado, los puertos abiertos encontrados y su función son los siguientes:

- **135/TCP:** este puerto es básico en los sistemas operativos Windows, debido a esto no se debe cerrar porque esto puede ocasionar que algunos programas o servicios que se estén ejecutando fallen, de igual forma este puerto puede ser víctima de ataques tipo denegación de servicio

  Recomendación: establecer una regla en el firewall donde este puerto no quede abierto al exterior y le sea imposible recibir el servicio de asistencia remota por el mismo, esto último puede variar si se realizar algún proceso externo de asistencia remota por este puerto caso contrario se debe realizar esta recomendación para evitar ataques de denegación de servicio o DOS

- **139/TCP:** en este puerto se ejecuta la NetBIOS, lo que permite interactuar con las distintas aplicaciones y servicios de la red donde se aloja el host, esto permite intercambiar archivos compartir recursos como impresoras y demás funciones que se realicen en red, al igual que el puerto 135 este no se puede cerrar debido a que recursos compartidos o en el caso de un servidor de archivos no se podrían utilizar correctamente.

  Recomendación: establecer una regla en el firewall donde este puerto no quede abierto al exterior a menos que este sea necesario según la arquitectura diseñada adicional a eso actualizar el antivirus y antimalware del servidor debido a que existen virus que atacan específicamente este puerto especialmente los de tipo gusano.

- **445/TCP:** este puerto ejecuta SMB (servidor de bloque de mensajes) que es la versión mejorada del puerto 139 NetBIOS, este puerto ejecuta las mismas funciones de intercambio de archivos y recursos compartidos en la red, permitiendo desactivar los puertos 139 sin problema a menos que exista alguna función o programa que los utilice, de igual forma este puerto también presenta vulnerabilidades que deben ser analizadas y corregidas.

  Recomendación: Aunque este puerto es otra versión del NetBIOS este sufre de vulnerabilidades a su protocolo SMB, una de las más conocidas es el eternal blue un virus que fue utilizado para atacar este puerto infectando la red de ramsonware y otro tipo de amenazas, al igual que en las demás recomendaciones se deben establecer reglas en el firewall que impidan salida o entrada a este puerto ya que debe ser de manejo solo interno de la red, así como tener actualizados los software antivirus, adicional a esto siendo el 455 una mejor versión del 139 este se podría desactivar lo que incrementa la seguridad y reduce posibles riesgos.

- **49152/TCP, 49153/TCP, 49154/TCP, 49156/TCP:** Desde el 49152 hasta el puerto 65535 son conocidos como puertos dinámicos estos están orientados a conexión al estilo P2P (persona a persona) por lo general no transmite ni manejan algún servido a menos que este se les programe y estarán disponibles cierto rango de puertos abiertos y a la escucha por defecto para este tipo de conexiones.

  Recomendación: si estos puertos no se están utilizando o han sido asignados a ningún programa o servicio que se esté ejecutando en el servidor se podrían desactivar sin problema, caso tal de que se necesitan o tengan que estar disponibles se debe crear el respectivo reglamento en el firewall que proteja estos puertos de accesos no autorizados debido a que estos estas en permanente escucha.

10.2 RESULTADOS OPENVAS

Con openvas se detectaron 3 vulnerabilidades 3 de tipo alto o riesgo alto y una de tipo medio o riesgo medio cuya descripción y recomendaciones para solucionar este tipo de vulnerabilidades están a continuación:

- **High (CVSS: 10.0)**
  NVT: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

  La explotación de esta vulnerabilidad puede ocasionar que acceso de atacantes remotos que ejecuten un bypass por medio de denegación de servicios o mecanismos de fuerza bruta, esta vulnerabilidad se basa en el error de validación de entrada al procesar las solicitudes de tipo SMB y se puede explotar por medio de un paquete SMB especialmente diseñado para esta vulnerabilidad, este aprovechamiento es gracias a un error al analizar los paquetes SMB durante la negociación en una conexión

  Solución: la solución a este problema no es del todo difícil, según los códigos de referencia CVE (common vulnerabilities and exposures) o vulnerabilidades y exposiciones comunes referenciado en los informes arrojados por Greenbone, este tipo de vulnerabilidad se encuentra parchada o solucionada por el fabricante en este caso Windows, entonces de debe realizar la actualización automática del sistema operativo en caso tal de tener desactivadas las actualizaciones se deben activar para correr este proceso y así corregir este problema

- **High (CVSS: 9.3)**
  NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

  Esta vulnerabilidad está relacionada con la anterior debido a un error paralelo al momento de la validación de entrada al procesar las solicitudes SMB que se pueden aprovechar para causar una explotación a través de un paquete SMB especialmente diseñado para este fin, para esta vulnerabilidad existe debido a un error en el análisis de peticiones en los paquetes SMB que ocasiona una corrupción de la memoria a través del diseñado para la explotar esta vulnerabilidad ayudando a filtrar al atacante mediante denegación de servicio y así obtener autenticación o escalamiento de privilegios según las intenciones del atacante, permitiendo ejecutar códigos maliciosos unas vez se tenga el acceso

  Solución: la solución a este problema tiene coincidencia con la solución anterior, según los códigos de referencia CVE (common vulnerabilities and exposures) o vulnerabilidades y exposiciones comunes referenciado en los informes arrojados por Greenbone, este tipo de vulnerabilidad se encuentra parchada o solucionada por el fabricante en este caso Windows, entonces de debe realizar la actualización automática del sistema operativo en caso tal de tener desactivadas las actualizaciones se deben activar para correr este proceso y así corregir este problema

- **Medium (CVSS: 5.0)**
  NVT: DCE/RPC and MSRPC Services Enumeration Reporting

  Esta vulnerabilidad está relacionada con los puertos dinámicos escaneados anteriormente con NMAP al igual que el apartado de Nmap, openvas también detecta la escucha constante de estos puertos como una vulnerabilidad de potencia media cuyo impacto ocasionaría que un atacante obtenga más información del host en este caso del servidor de forma remota

  Recomendación: se aconseja realizar filtrado programado a estos puertos con programas de detección de amenazas firewalls o relacionados que puedan ejercer esta función, si estos puertos no están siendo usados por ningún programa o servicio y pueden ser desactivados total o parcialmente es recomendable ejecutar esta acción para evitar posibles riesgos futuros.

CONCLUSIONES

Las evidencias en el análisis de vulnerabilidades realizadas en el servidor de pruebas demuestran hallazgos de vulnerabilidades que hasta esa fecha eran desconocidas por el departamento de sistemas del hospital de tocaima, esto demuestra que no importa el tipo de infraestructura que se tenga ningún sistema es perfecto o infalible, y puede estar expuesto a posibles intrusiones o fallos que pueden causar colapso en la prestación de un servicio.

Encontrar evidencias de vulnerabilidades en cualquier tipo de infraestructura en este caso un servidor de pruebas, es una alerta a tomar en cuenta para cualquier administrador de sistemas o líder de departamento de sistemas, este tipo de procesos hace replantear las practicas realizadas referentes a seguridad informática y como estas deben evolucionar así como las amenazas y vulnerabilidades cambian con el pasar del tiempo volviendo más robustos todos los objetos que integran una infraestructura.

Por otro lado tenemos una gran y versátil herramienta de análisis de vulnerabilidades OPENVAS, esta herramienta demostró una gran flexibilidad al momento de ejecutar el análisis ofreciendo muy buenas opciones para usuarios principiantes que están iniciando en este tipo de actividades de seguridad informática, esto demuestra que una herramienta de naturaleza gratuita como lo es openvas puede hacerle frente a herramientas de pago y ofrecer resultados de calidad.

Otra de las herramientas que fueron de gran ayuda fue la suite de seguridad informática KALILINUX, al igual que openvas, esta distribución es totalmente gratuita y sirve como complemente perfecto para realizar pentesting reconociendo posibles fallas a diferentes niveles y objetivos que posiblemente los analizadores de vulnerabilidades puedan pasar por alto, lo que demuestra que al igual que la infraestructuras los métodos de análisis no son perfectos y pueden necesitar complementos adicionales para dar una visión adicional al escenario analizado.

Posteriormente tenemos el informe de vulnerabilidades arrojado por GREENBONE, que es el asistente integrado de openvas, este informe fue la herramienta fundamental para generar las recomendaciones a tener en cuenta para el proceso de hardening, en el están todas la

amenazas clasificadas a detalle y como mitigarlas, adicionalmente greenbone incluyo links a comunidades que contienen información adicional sobre las vulnerabilidades encontradas en relación a lo anterior al igual que kalilinux, greenbone es un complemento perfecto una herramienta robusta y precisa que ofrece justo lo que se necesitaba para este tipo de procesos.

Por ultimo se puede concluir que la revisión de vulnerabilidades en una infraestructura informática ya sea en su totalidad o a un solo componente que la integra como lo fue el servidor de pruebas y sin importar de que entidad u organización se trate, debe ser un proceso estandarizado y obligatorio que genere un posterior hardening a la infraestructura, documentando todos los resultados obtenidos para conocer qué tipo de vulnerabilidades fueron encontradas y como mitigarlas.

BIBLIOGRAFÍA

1. ANDRÉS, R. (2016). Qué es Kali Linux y qué puedes hacer con él. [pagina web] ComputerHoy. Disponible en:: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671 [Consulta: 15 Nov. 2018].

2. APRENDIZDESYSADMIN.COM (2018). *Guía Hardening Instalación del Sistema*. [pagina web] Aprendiz de sysadmin. Disponible en:: https://aprendizdesysadmin.com/guia-hardening-instalacion-del-sistema/[Consulta: 17 Oct. 2018].

3. AVILA, F. (2018). Scanner de vulnerabilidades (Herramientas #2) | Security Hack Labs. [pagina web] Security Hack Labs. Disponible en:: https://securityhacklabs.net/articulo/escaner-de-vulnerabilidades-herramientas-2 [Consulta: 12 Dec. 2018].

4. BORNIK, S. (N.D.). Pruebas de penetración Para principiantes: 5 herramientas Para empezar. [pagina web] Revista.seguridad.unam.mx. Disponible en:: https://revista.seguridad.unam.mx/print/2233 [Consulta: 12 Dec. 2018].

5. CABALLERO, A. (N.D.). Escaneo de Vulnerabilidades Externo utilizando OpenVAS | Alonso Caballero Quezada / ReYDeS. [pagina web] Reydes.com. Disponible en:: http://www.reydes.com/d/?q=Escaneo_de_Vulnerabilidades_Externo_utilizando_OpenVAS [Consulta: 12 Dec. 2018].

6. CASTRO, I. (2018). *¿Qué es un Análisis de Vulnerabilidades Informáticas?*. [pagina web] Blog de #NextGenSecurity. Disponible en:: http://blog.cerounosoftware.com.mx/que-es-un-analisis-de-vulnerabilidades-inform%C3%A1ticas [Consulta: 17 Oct. 2018].

7. CLASIFICACIONDE. (2018). Clasificación de los hospitales - ¿Cómo se clasifican?. Retrieved from https://www.clasificacionde.org/hospitales/
8. cursodehackers.com (2017). Curso de hackers - Escaner Nessus de vulnerabilidades. [pagina web] Cursodehackers.com. Disponible en:: http://www.cursodehackers.com/nessus.html [Consulta: 15 Nov. 2018].

9. DESCARGAS.PNTIC.MEC.ES (2018). *Vulnerabilidades de un sistema informático | Seguridad Informática*. [pagina web] Descargas.pntic.mec.es. Disponible en:: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html [Consulta: 17 Oct. 2018].

10. DRAGONJAR.ORG (2018). Hardening, Conceptos básicos. [pagina web] Dragonjar.org. Disponible en:: https://www.dragonjar.org/hardening-conceptos-basicos.xhtml.

11. E.S.E. HOSPITAL MARCO FELIPE AFANADOR DE TOCAIMA (2019). *Política de Tratamiento de Datos*. [pagina web] Hmfa-tocaima-cundinamarca.gov.co. Disponible en:: http://www.hmfa-tocaima-cundinamarca.gov.co/politicas-y-lineamientos/politica-de-tratamiento-de-datos [Consulta: 18 Mar. 2019].

12. ECURED.CU (N.D.). Kali linux. [pagina web] EcuRed. Disponible en:: https://www.ecured.cu/Kali_linux [Consulta: 17 Nov. 2018].

13. EL TIEMPO (2018). EN 2015, cibercrimen generó pérdidas por US$ 600 millones en Colombia. [pagina web] El Tiempo. Disponible en:: https://www.eltiempo.com/archivo/documento/CMS-16493604 [Consulta: 10 Oct. 2018].

14. EL-NACIONAL.COM (2017). Los 10 incidentes de seguridad informática más importantes del último año. [pagina web] El Nacional. Disponible en:: http://www.el-nacional.com/noticias/empresas/los-incidentes-seguridad-informatica-mas-importantes-del-ultimo-ano_75387 [Consulta: 27 Nov. 2018].

15. GARCIA, U. (2017). ¿Qué es una vulnerabilidad?. [pagina web] Blog de #NextGenSecurity. Disponible en:: http://blog.cerounosoftware.com.mx/qu%C3%A9-es-una-vulnerabilidad [Consulta: 18 Nov. 2018].

16. GÓMEZ, A. (2018). *Anexo III Análisis y Gestión de Riesgos en un Sistema Informático*. [pagina web] Academia.edu. Disponible en:: https://www.academia.edu/5971566/Anexo_III_An%C3%A1lisis_y_Gesti%C3%B3n_de_Riesgos_en_un_Sistema_Inform%C3%A1tico [Consulta: 17 Oct. 2018].

17. HEIDEGGER, Z. (2011). Manual práctico de OpenVAS en Español | Blackploit [PenTest]. [pagina web] Blackploit.com. Disponible en:: https://www.blackploit.com/2011/04/manual-practico-de-openvas-open.html [Consulta: 27 Nov. 2018].

18. PNTIC.MEC.ES (N.D.). Vulnerabilidades de un sistema informático | Seguridad Informática. [pagina web] Descargas.pntic.mec.es. Disponible en:: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html [Consulta: 27 Nov. 2018].

19. FACILITAMOS.CATEDU.ES (N.D.). Práctica con Nmap/Zenmap | Unidad Didáctica: 7 Propuesta Didáctica: Instalación/configuración de los equipos de red. [pagina web] Facilitamos.catedu.es. Disponible en:: http://facilitamos.catedu.es/previo/fpinformatica/INFOR_U6_1_tcp-ipZIP/prctica_con_nmapzenmap.html [Consulta: 27 Nov. 2018].

20. INFOSEGUR (2018). Vulnerabilidades | Seguridad Informática. [pagina web] Infosegur.wordpress.com. Disponible en:: https://infosegur.wordpress.com/tag/vulnerabilidades/ [Consulta: 18 Nov. 2018].

21. INFOSEGUR.WORDPRESS.COM (2013). Vulnerabilidades | Seguridad Informática. [pagina web] Infosegur.wordpress.com. Disponible en:: https://infosegur.wordpress.com/tag/vulnerabilidades/ [Consulta: 27 Nov. 2018].

22. KHEPRI, W. (2018). Las 25 mejores herramientas de Kali Linux – William Khepri – Medium. [pagina web] Medium. Disponible en:: https://medium.com/@williamkhepri/las-25-mejores-herramientas-de-kali-linux-b8c2a92f2ab4 [Consulta: 12 Dec. 2018].

23. L4BS, S. (2016). Snifer@L4b's: Listado Completo Herramientas en Kali Linux. [pagina web] Snifer@L4b's. Disponible en:: https://www.sniferl4bs.com/2014/03/listado-completo-herramientas-en-kali.html [Consulta: 17 Nov. 2018].

24. LÓPEZ, D. (N.D.). Evolución de la Seguridad Informática | Grupo Control. [pagina web] Grupocontrol.com. Disponible en:: https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica [Consulta: 26 Nov. 2018].

25. MARTÍNEZ, E. (2017). 7 de los ciberataques más famosos de la historia. [pagina web] Icorp.com.mx. Disponible en:: http://www.icorp.com.mx/blog/ciberataques-mas-famosos/ [Consulta: 27 Nov. 2018].

26. MENDOZA, M. (2014). Cómo utilizar OpenVAS para la evaluación de vulnerabilidades. [pagina web] WeLiveSecurity. Disponible en:: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/ [Consulta: 15 Nov. 2018].

27. MENDOZA, M. (2014). Cómo utilizar OpenVAS para la evaluación de vulnerabilidades. [pagina web] WeLiveSecurity. Disponible en:: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/ [Consulta: 27 Nov. 2018].

28. MIFSUD, E. (2018). *MONOGRÁFICO: Introducción a la seguridad informática - Vulnerabilidades de un sistema informático | Observatorio Tecnológico*. [pagina web] Recursostic.educacion.es. Disponible en:: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3 [Consulta: 17 Oct. 2018].

29. MURCIA, C. (2003). Introducción a Nmap. [pagina web] Maestros del Web. Disponible en:: http://www.maestrosdelweb.com/nmap/ [Consulta: 12 Dec. 2018].

30. NMAP.ORG (N.D.). Guía de referencia de Nmap (Página de manual) |. [pagina web] Nmap.org. Disponible en:: https://nmap.org/man/es/index.html [Consulta: 12 Dec. 2018].

31. OTEGUI, A. (2018). *Herramientas de análisis de vulnerabilidades*. [pagina web] Es.slideshare.net. Disponible en:: https://es.slideshare.net/alejandro_otegui96/herramientas-de-anlisis-de-vulnerabilidades-81021908 [Consulta: 17 Oct. 2018].

32. OTEGUI, A. (2018). Herramientas de análisis de vulnerabilidades. [pagina web] Es.slideshare.net. Disponible en:: https://es.slideshare.net/alejandro_otegui96/herramientas-de-anlisis-de-vulnerabilidades-81021908 [Consulta: 17 Oct. 2018].

33. PARAISOLINUX.COM (2017). Que es y como usar NMAP - Paraiso Linux. [pagina web] Paraiso Linux. Disponible en:: https://paraisolinux.com/que-es-y-como-usar-nmap/ [Consulta: 12 Dec. 2018].

34. PÉREZ, I. (2015). Auditando con Nmap y sus scripts para escanear vulnerabilidades. [pagina web] WeLiveSecurity. Disponible en:: https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/ [Consulta: 27 Nov. 2018].

35. PINILLA, L. (2015). Que es y Como usar Nmap. [pagina web] Es.slideshare.net. Disponible en:: https://es.slideshare.net/luispinilla96/que-es-y-como-usar-nmap [Consulta: 12 Dec. 2018].

36. PRANDINI, P. (2018). *Vulnerabilidades, amenazas y riesgo en "texto claro" | Magazcitum*. [pagina web] Magazcitum.com.mx. Availableat:http://www.magazcitum.com.mx/?p=2193[Consulta: 17 Oct. 2018].

37. REDACCIÓN EL TIEMPO. (2018). CLASIFICACION DE LOS HOSPITALES. Retrieved from https://www.eltiempo.com/archivo/documento/MAM-627858.

38. SEGUINFO.WORDPRESS.COM (2007). ¿Qué es Nmap?. [pagina web] Seguridad Informática. Disponible en:: https://seguinfo.wordpress.com/2007/06/27/%C2%BFque-es-nmap/ [Consulta: 27 Nov. 2018].

39. SEGUINFO.WORDPRESS.COM (2018). *Proceso de Hardening*. [pagina web] Seguridad Informática. Disponible en:: https://seguinfo.wordpress.com/2012/04/03/proceso-de-hardening/.

40. SEGURIDAD, N. (2018). *¿Cómo hacer análisis de vulnerabilidades informáticas?*. [pagina web] Noticiasseguridad.com. Disponible en:: http://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/

41. SEGURIDAD, N. (2018). ¿Cómo hacer análisis de vulnerabilidades informáticas?. [pagina web] Noticiasseguridad.com. Disponible en:: http://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/

42. SMARTEKH, G. (2018). *¿QUÉ ES HARDENING?*. [pagina web] Blog.smartekh.com. Disponible en: http://blog.smartekh.com/que-es-hardening.

43. SOLVETIC.COM (2018). Hardening seguridad de servidores y sistemas operativos. [pagina web] Solvetic. Disponible en:: https://www.solvetic.com/tutoriales/article/1875-hardening-seguridad-de-servidores-y-sistemas-operativos/.

44. TECNOLOGIA-INFORMATICA.COM (N.D.). Vulnerabilidades informáticas - Tecnología & Informática. [pagina web] Tecnología & Informática. Disponible en:: https://tecnologia-informatica.com/vulnerabilidades-informaticas/ [Consulta: 27 Nov. 2018].

45. THESECURITYSENTINEL.ES (2018). Curso de Hardening de Servidores Windows - The Security Sentinel. [pagina web] The Security Sentinel. Disponible en:: https://thesecuritysentinel.es/curso/hardening-servidores-windows/

46. TRUST NETWORK (2018). Análisis de Vulnerabilidades. [pagina web] Trust-network.net. Disponible en:: http://www.trust-network.net/blog-trustnet/analisis-de-vulnerabilidades [Consulta: 13 Dec. 2018].

47. UNIVERSIDADVIU.COM (2018). Vulnerabilidad informática, tipos y debilidades principales | VIU. [pagina web] Universidadviu.com. Disponible en:: https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/ [Consulta: 18 Nov. 2018].

48. UNIVERSIDADVIU.COM (2018). Vulnerabilidad informática, tipos y debilidades principales | VIU. [pagina web] Universidadviu.com. Disponible en:: https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/ [Consulta: 27 Nov. 2018].

49. VILLANUEVA, C. (2018). Hardening de un Sistema Operativo de Red. [pagina web] https://www.lawebdelprogramador.com. Disponible en:: https://www.lawebdelprogramador.com/pdf/10383-Hardening-de-un-Sistema-Operativo-de-Red.html.

50. VILLAR, M. (2018). metodologías y herramientas de ethical hacking. retrieved from https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html.

Anexos

Anexo 1 Solicitud de permiso aprobada por el gerente del hospital para realizar el análisis de vulnerabilidades

Tocaima, 2 de mayo de 2019

Doctor
CARLOS ANDRÉS PRADA ÁLVAREZ
Gerente
ESE HOSPITAL MARCO FELIPE AFANADOR
Ciudad

Cordial saludo, yo DIEGO FRANCISCO BALLÉN LEÓN identificado con la cedula de ciudadania 1.076.626.149 de Tocaima, actual estudiante de posgrado de la especialización de seguridad informática de la universidad nacional abierta y a distancia UNAD, solicito a usted el permiso para poder realizar las pruebas relacionadas con mi proyecto de grado bajo la opción de monografia, en el servidor de **pruebas** de la E.S.E. Hospital Marco Felipe Afanador de Tocaima, las pruebas que se realizaran en dicho servidor consistirán en un análisis de vulnerabilidades informáticas, cuyos resultados obtenidos serán analizados y servirán para implementar un proceso de Hardening en el servidor" proceso de endurecimiento y refuerzo a nivel de hardware o software para eliminar, corregir y evitar posibles vulnerabilidades y fallos relacionados con la seguridad informática".

De igual forma me comprometo y garantizo según la actual política de tratamiento de datos de su institución relacionada en la resolución 075 del 2019, que se preservara la integridad disponibilidad e integridad de las bases de datos asociadas a dicho servidor garantizando que en ningún momento se manipulara, accederá, copiara sin permiso, alterara o se realizara alguna acción a esta, y que todo el proceso de análisis se realizara bajo la supervisión y control del personal perteneciente al departamento de sistemas de su institución.

Agradezco su atención

Atentamente,

Diego Francisco Ballén león
C.C. 1.075.626.149

Aprobación:

Anexo 2 Informe Openvas

Scan Report

May 6, 2019

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 192.168.137.184". The scan started at Mon May 6 19:15:48 2019 UTC and ended at Mon May 6 19:26:01 2019 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview 2

2 Results per Host 2

2.1 192.168.137.184 2

2.1.1 High 445/tcp 2

2.1.2 Medium 135/tcp 4

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.137.184	2	1	0	0	0
Total: 1	2	1	0	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 3 results selected by the filtering described above. Before filtering there were 14 results.

2 Results per Host

2.1 192.168.137.184

Host scan start	Mon May 6 19:16:01 2019 UTC
Host scan end	Mon May 6 19:26:01 2019 UTC

Service (Port)	Threat Level
445/tcp	High
135/tcp	Medium

2.1.1 High 445/tcp

2 Results per Host

2.1 192.168.137.184

Host scan start	Mon May 6 19:16:01 2019 UTC
Host scan end	Mon May 6 19:26:01 2019 UTC

Service (Port)	Threat Level
445/tcp	High
135/tcp	Medium

2.1.1 High 445/tcp

High (CVSS: 10.0)
NVT: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS10-012.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service or bypass the authentication mechanism via brute force technique.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Windows 7
Microsoft Windows 2000 Service Pack and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2003 Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior

Vulnerability Insight
- An input validation error exists while processing SMB requests and can be exploited to cause a buffer overflow via a specially crafted SMB packet.
- An error exists in the SMB implementation while parsing SMB packets during the Negotiate phase causing memory corruption via a specially crafted SMB packet.
- NULL pointer dereference error exists in SMB while verifying the 'share' and 'servername' fields in SMB packets causing denial of service.
- A lack of cryptographic entropy when the SMB server generates challenges during SMB NTLM authentication and can be exploited to bypass the authentication mechanism.

Vulnerability Detection Method
Details: `Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)`
OID:1.3.6.1.4.1.25623.1.0.902269
Version used: `2019-05-03T10:54:50+0000`

References
`CVE: CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231`
`Other:`
`URL:http://secunia.com/advisories/38510/`
`URL:http://support.microsoft.com/kb/971468`
`URL:http://www.vupen.com/english/advisories/2010/0345`
`URL:http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx`

Vulnerability Detection Method

Details: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)
OID:1.3.6.1.4.1.25623.1.0.902269
Version used: 2019-05-03T10:54:50+0000

References

CVE: CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231
Other:
URL:http://secunia.com/advisories/38510/
URL:http://support.microsoft.com/kb/971468
URL:http://www.vupen.com/english/advisories/2010/0345
URL:http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

. . . continues on next page . . .

... continued from previous page ...

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: `2019-05-03T10:54:50+0000`

References
```
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,
↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
  URL:https://support.microsoft.com/en-in/kb/4013078
   URL:https://technet.microsoft.com/library/security/MS17-010
   URL:https://github.com/rapid7/metasploit-framework/pull/8167/files
```

References

CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, ↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
URL:https://support.microsoft.com/en-in/kb/4013078
URL:https://technet.microsoft.com/library/security/MS17-010
URL:https://github.com/rapid7/metasploit-framework/pull/8167/files

[return to 192.168.137.184]

2.1.2 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary

. . . continues on next page . . .

... continued from previous page ...

```
      Annotation: IPSec Policy agent endpoint
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
      Endpoint: ncacn_ip_tcp:192.168.137.184[49163]
      Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: $Revision: 6319 $

[return to 192.168.137.184]