IDENTIFICACION DE VULNERABILIDADES DE LA RED LAN DEL BUQUE OCEANOGRÁFICO DE LA AUTORIDAD COLOMBIANA A TRAVÉS DE LAS HERRAMIENTAS DE PRUEBAS DE PENTESTING

AYDEE MERCEDES VIVER RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CALI

2016

IDENTIFICACION DE VULNERABILIDADES DE LA RED LAN DEL BUQUE OCEANOGRÁFICO DE LA AUTORIDAD COLOMBIANA A TRAVÉS DE LAS HERRAMIENTAS DE PRUEBAS DE PENTESTING

AYDEE MERCEDES VIVER RAMIREZ

Trabajo de grado como requisito para optar por el título de:
Especialista en Seguridad Informática

Ing. Martin Camilo Cancelado Ruiz
Asesor de proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2016

Nota de aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Santiago de Cali, Noviembre de 2016

Este trabajo de grado se lo dedico a Dios y a la Virgen quienes me han dado su protección a lo largo de los años y de mi carrera.

Igualmente a mi madre y mi familia quienes han sido mi motivación y fuerza para lograr todas las metas propuestas.

A mi esposo quien me ha acompañado, entendido y apoyado para llevar a feliz término este nuevo peldaño.

AGRADECIMIENTOS

Mi más sincero mensaje de agradecimiento a la Autoridad Marítima Colombiana por brindarme el apoyo necesario para emprender esta especialización que hoy culmino con éxitos.

Igualmente agradecer a mi madre, a mis sobrinas quienes me han impulsado para ser cada día mejor.

A Darwin Fernández y Alonso Mondragón por su incondicional apoyo cada vez que los necesite.

A todos mil gracias.

CONTENIDO

pág.

INTRODUCCIÓN 12

1. TÍTULO 13

2. DEFINICIÓN DEL PROBLEMA 14
2.1 PLANTEAMIENTO DEL PROBLEMA 14
2.2 FORMULACIÓN DEL PROBLEMA 15

3. JUSTIFICACIÓN 16

4. OBJETIVOS 17
OBJETIVO GENERAL 17
OBJETIVOS ESPECÍFICOS 17

5. MARCO REFERENCIAL 18
5.1 ANTECEDENTES 18
5.2 MARCO TEÓRICO 18
5.2.1 Seguridad Informática. 20
5.2.2 Principios de Seguridad Informática. 20
5.2.3 Red de datos. 20
5.2.4 Vulnerabilidad. 20
5.2.5 Ataques informáticos. 21
5.3 MARCO CONCEPTUAL 21
5.4 MARCO LEGAL 23
5.4.1 Ley 1273 de 2009. 23
5.4.2 Documento Conpes 3701. 24
5.4.3 Norma Técnica Colombiana NTC 5254. 25

6. DISEÑO METODOLÓGICO 26
6.1 CLASE DE INVESTIGACIÓN 27
6.2 ÁREA DE CONOCIMIENTO GENERAL Y ESPECÍFICA 27
6.3 INVESTIGADORES Y/O COLABORADORES 27
6.4 PRODUCTOS A ENTREGAR 27
6.5 ALCANCES DEL PROYECTO O DELIMITACIÓN 28
6.6 POBLACIÓN 28
6.7 MUESTRA 28

7. RECURSOS DISPONIBLES 29
7.1 RECURSO HUMANO 29
7.2 RECURSO FÍSICO Y FINANCIERO 29
7.3 RECURSO TÉCNICO 30

8. RESULTADOS Y DISCUSIÓN 31
8.1 VERIFICACIÓN DE ESTADO DE LA RED LAN DEL BUQUE OCEANOGRÁFICO A.R LIBERTAD PARA REALIZAR RECOMENDACIONES EN CUANTO A SEGURIDAD INFORMÁTICA 31
8.1.1 Verificación física de la red. 31
8.1.2 Verificación lógica de la red. 38
8.1.3 Controles y/o medidas establecidas para la seguridad de la red. 39
8.2 APLICACIÓN DE HERRAMIENTA DE PENTESTING, PARA REALIZAR PRUEBAS DE CAJA BLANCA E IDENTIFICAR LAS VULNERABILIDADES SOBRE LA RED LAN DEL BUQUE OCEANOGRÁFICO A.R LIBERTAD 40
8.2.1 Recolección de información. 40
8.2.1.1 Elementos activos de la red. 40
8.2.1.2 Equipos de cómputo identificados. 40
8.2.1.3 Sistemas operativos identificados. 41
8.2.1.4 Topología de la red. 41
8.2.1.5 Medio de transmisión. 42
8.2.1.6 Conexión a la red. 42
8.2.1.7 Puntos estructurados en la red. 42
8.2.1.8 Puestos de trabajo instalados actualmente. 42
8.2.1.9 Restricciones establecidas para uso de la red. 42

8.2.1.10 Privilegios establecidos para uso de la red. 42
8.2.1.11 Usuarios que interactúan con la red LAN, modalidad, incluye configuración. 42
8.2.2 Planificación. 43
8.2.3 Ejecución y evidencia de resultados obtenidos con herramientas de pentesting. 43
8.2.3.1 Herramientas de Pestesting utilizadas. 43
8.2.3.2 Revisión de antivirus, malware y otros métodos de defensa, donde se pueda identificar su efectividad y actualización. 43
8.2.3.3 Revisión de puertos abiertos, privilegios que conceda la configuración de la máquina y evidencia de resultados obtenidos con Herramientas de Pentesting. 44
8.2.3.4 Aplicación de la herramienta GFI LanGuard 2015 para identificar posibles vulnerabilidades. 49
8.3 REALIZAR UN ANALISIS COMPLETO Y DETALLADO SOBRE EL ESTADO DE LA RED LAN DEL BUQUE OCEANOGRÁFICO A.R LIBERTAD. 54
8.3.1 Análisis de hallazgos sobre la red LAN del buque oceanográfico A.R LIBERTAD. 54
8.3.2 Recomendaciones de acciones o controles que se deben realizar para reducir ataques por vulnerabilidades 58
8.3.2.1 Red estructurada. 59
8.3.2.2. Métodos de protección. 61
8.4 POLÍTICAS DE SEGURIDAD PROPUESTAS. 62

9. RESULTADOS E IMPACTOS 73
9.1 RESULTADOS 73
9.2 IMPACTOS 74
9.3 AVANCE DE RESULTADOS. 76

10. DIVULGACION 80

11. CRONOGRAMA 81

BIBLIOGRAFÍA 82

LISTA DE TABLAS

pág.

Tabla 1. Muestra seleccionada de la red LAN del buque oceanográfico A.R LIBERTAD 28

Tabla 2. Recurso físico y financiero 29

Tabla 3. Elementos activos de la red LAN del buque oceanográfico A.R LIBERTAD 40

Tabla 4. Equipos de cómputo identificados en la red LAN del buque oceanográfico A.R LIBERTAD 41

Tabla 5. Métodos de defensa 43

Tabla 6. Resumen de vulnerabilidades encontradas 76

LISTA DE FIGURAS

pág.

Figura 1. Diagrama de la red de datos del buque oceanográfico A.R. LIBERTAD 31
Figura 2. Canaleta externa de la red de datos del A.R. LIBERTAD 32
Figura 3. Conexión del cable UTP al Jack de la caja de conexión 33
Figura 4. Organización cable UTP y Cable eléctrico en la canaleta externa 33
Figura 5. Organización cable UTP en el Patch panel (lado izquierdo) del rack de comunicaciones 34
Figura 6. Organización cable UTP en el Patch panel (lado derecho) del rack de comunicaciones 34
Figura 7. Marcación inexistente en el Patch panel marca Quest 36
Figura 8. Marcación en el Patch panel marca QPCOM 36
Figura 9. Marcación del cableado UTP 37
Figura 10. Monitorización Red LAN del A.R. LIBERTAD 39
Figura 11. Se identifican los puertos abiertos de los equipos correspondientes a la IP 192.168.0.1 y 192.168.0.2 44
Figura 12. Se identifican los puertos abiertos de los equipos correspondientes a la IP 192.168.0.3 y 192.168.0.4 45
Figura 13. Se identifican los puertos abiertos del equipo correspondientes a la IP 192.168.0.100 46
Figura 14. Esquema de la topología de red identificada por Nmap con los equipos que se seleccionados en la de muestra 46
Figura 15. Detalles del host 192.168.0.1 47
Figura 16. Detalles del host 192.168.0.2 47
Figura 17. Detalles del host 192.168.0.3 48
Figura 18. Detalles del host 192.168.0.4 48
Figura 19. Detalles del host 192.168.0.100 49
Figura 20. Identificación de puertos abiertos host 192.168.0.100 50
Figura 21. Nivel de vulnerabilidad de la red 50

Figura 22. Evaluación de vulnerabilidades encontradas en los equipos de la red 51
Figura 23. Informe de vulnerabilidades por categorías 51
Figura 24. Informe de vulnerabilidades categoría media 52
Figura 25. Informe de vulnerabilidades categoría baja 52
Figura 26. Informe de vulnerabilidades potenciales 53
Figura 27. Informe de vulnerabilidades por falta de actualizaciones del sistema 53
Figura 28. Resumen de vulnerabilidades encontradas 78

INTRODUCCIÓN

En la actualidad se puede observar como la tecnología, las comunicaciones, la informática y el internet, se han convertido en una necesidad, poco a poco han ido ganando terreno siendo hoy en día una parte fundamental desde toda perspectiva; haciendo énfasis en el sector institucional y/o empresarial vemos como para adelantar la mayoría de las funciones se requiere de la informática y todo lo que implica tecnología.

También es cierto que cada día las naciones buscan a través de sus respectivas flotas navales fortalecer su poder marítimo, Colombia no es la excepción, para ello cuenta con buques con diferentes funciones, entre ellas la oceanografía, estos buques tienen una función privilegiada ya que a través de sus levantamientos de información oceanográfica logran obtener datos indispensables para la realización de cartas marítimas, estas cartas son administradas y distribuidas por la Autoridad Marítima y están a disposición de todas las embarcaciones que navegan por mares y puertos Colombianos, estas cartas son la guía completa para que su tránsito se realice con total tranquilidad y seguridad; Igualmente logran la búsqueda, ubicación y rescate de especies naufragas como es el caso del Galeón San José; realizan estudios que permiten determinar las corrientes marinas estas a su vez sirven para determinar la ocurrencia de un Tsunami para que las entidades correspondientes generen alertas y puedan prevenir desastres en las costas tanto de Colombia como del mundo.

Colombia cuenta con buques oceanográficos muy bien equipados para su investigación científica sin embargo no sucede lo mismo en cuanto al equipamiento para proteger la información digital que se está obteniendo, resultado de las exploraciones marinas; teniendo en cuenta la importancia que tiene esta información para el país, se realizará una serie de pruebas que permitan verificar el nivel de seguridad con que cuenta la red LAN de uno de estos buques oceanográficos de la Autoridad Colombiana con el fin de efectuar un análisis y dar recomendaciones para que los altos mandos tengan una herramienta de evaluación y una base para la toma de decisiones que vayan en pro de la seguridad informática de los elementos activos de la red y de esta manera se proteja la integridad, disponibilidad y confiabilidad de la información que obtienen.

1. TÍTULO

IDENTIFICACION DE VULNERABILIDADES DE LA RED LAN DEL BUQUE OCEANOGRÁFICO DE LA AUTORIDAD COLOMBIANA A TRAVÉS DE LAS HERRAMIENTAS DE PRUEBAS DE PENTESTING.

2. DEFINICIÓN DEL PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

Actualmente la Autoridad Marítima Nacional cuenta con varios buques oceanográficos, estos buques se encargan de tareas tan importantes como el levantamiento de información batimétrica para la realización de las cartas de navegación, las cuales son utilizadas por todas las motonaves ya sean nacionales o extranjeras que van a ingresar o a realizar tránsito por uno de los puertos navegables en Colombia.

También tienen como función la ubicación precisa de las boyas que son un pilar fundamental en la navegación, ya que estos instrumentos indican la ruta a seguir para que todas las embarcaciones y en especial las de gran tamaño y calado tengan una navegación segura y no sufran un siniestro marítimo.

Igualmente realizan el levantamiento de información para el estudio y análisis del subsuelo marítimo, estos estudios son utilizados para temas tan importantes y fundamentales para el país como son el descubrimiento de especies naufragas.

Uno de esos buques es el A.R LIBERTAD, el cual por un tiempo fijo de un año estará asignado a tareas específicas en la jurisdicción del Océano Pacifico Colombiano.

Este buque cuenta con equipos de cómputo dentro de una red de datos, esta red permite intercomunicación entre los equipos, dispositivos y navegación de los mismos, algunos de estos equipos son sensibles por la información que se almacena y por la importancia que reviste la misma para los intereses institucionales y gubernamentales. Sin embargo se evidencia la falta de seguridad de dicha información, ya que las medidas adoptadas para la protección de la red son casi nulas y en algunos casos se evidencian equipos que no cuentan con ninguna medida de seguridad, lo que origina una red de datos totalmente vulnerable frente a una potencial amenaza que arroje como consecuencias, la

alteración, robo o daño de la información lo cual va a redundar en posibles fallas y retrasos en el servicio que debe prestar la Autoridad Marítima al sector marítimo colombiano y al sector internacional que hace tránsito por nuestros mares. Estas fallas y retrasos pueden incluso acarrear sanciones internacionales para cualquier nación incluida Colombia

2.2 FORMULACIÓN DEL PROBLEMA

Se considera que la red de datos del buque oceanográfico A.R LIBERTAD es segura?

3. JUSTIFICACIÓN

Los ataques a la seguridad de las redes LAN son tema de todos los días, ninguna empresa, institución, gobierno están exentos, incluso las grandes empresas y gobiernos con tecnología de punta han sido vulneradas por ataque a sus redes informáticas y después de mucho tiempo de realizados los ataques, aún están sufriendo las consecuencias.

Es por ello que se ha convertido en una práctica muy habitual y casi necesaria el de realizar verificaciones de las redes de datos a través de herramientas de Pentesting con el fin de determinar el nivel de vulnerabilidad con que cuenta tanto la red como los equipos que hace parte de ella.

La red LAN del buque oceanográfico A.R LIBERTAD no es la excepción, esta red y los equipos de cómputo presentan una serie de fallas que pueden permitir la realización de ataques informáticos, lo que puede traer consigo espionaje, robo, alteración o daño en la información obtenida en los trabajos realizados, perjudicando seriamente los intereses del país.

La implementación de herramientas de Pentesting sobre la red LAN del buque oceanográfico A.R LIBERTAD, servirán para determinar las vulnerabilidades presentes a fin de determinar procedimientos o políticas a implementar para salvaguardar la información y los equipos que hagan parte de la red. Igualmente servirá de ejercicio para auditar su nivel de seguridad informática y permitirá al administrador de la red conocer ataques de los cuales pueda estar siendo víctima e identificar y analizar vulnerabilidades para tomar acciones correspondientes que permitan combatirlas, extremar medidas y contar con una red mucho más segura.

Igualmente permitirá obtener información para ser suministrada al comandante del buque y a la oficina de informática de la sede central para elevar el nivel de conciencia acerca de la importancia de la seguridad de las redes y de la información y de esta manera el administrador de la red tendrá mayor apoyo en el desempeño de su labor.

4. OBJETIVOS

OBJETIVO GENERAL

Determinar la cantidad de vulnerabilidades existentes de la red LAN con que cuenta el buque oceanográfico A.R LIBERTAD, perteneciente a la Autoridad Marítima Nacional

OBJETIVOS ESPECÍFICOS

- Verificar el estado de la red LAN del buque oceanográfico A.R LIBERTAD para realizar recomendaciones en cuanto a seguridad informática.

- Aplicar Herramientas de Pentesting para realizar pruebas de caja blanca, e identificar las vulnerabilidades existentes sobre la red LAN del buque oceanográfico A.R LIBERTAD.

- Realizar un análisis completo y detallado sobre el estado de la red LAN del buque oceanográfico A.R LIBERTAD con el fin de presentar recomendaciones basados en los hallazgos que se realicen; estas recomendaciones estarán enfocadas en acciones o controles que se deben realizar para reducir ataques por vulnerabilidades que se puedan presentar en la red LAN.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

El Ministerio de Defensa de cada País, desde su fuerza naval, tienen a su cargo temas importantes y vitales para salvaguardar intereses marítimos nacionales e internacionales, es por ello que cuentan dentro de su flota naval con buques oceanográficos, estos buques inicialmente estaban dotados de equipos especializados en investigación marina, hoy en día se puede apreciar cómo surge la necesidad que contar con redes de datos que les permita interconectar tanto los equipos de investigación marina como los equipos de cómputo y el parque computacional necesario para facilitar y mejorar el almacenamiento y procesamiento de datos.

Es el caso de la Armada Ecuatoriana la cual cuenta con el buque de investigación “ORION”, en el año 2008, realizaron un procedimiento de modernización de esta nave, esa modernización incluyó la instalación de una red de datos LAN, esta red cuenta con 22 puntos estructurados, en el año 2013 teniendo en cuenta una serie de novedades se detecta que la red LAN no es óptima ya que dificulta el intercambio de información, esto ocasiona un incremento en el tiempo estimado para la realización de trabajos asignados, por ello vieron la necesidad de gestionar el mantenimiento y verificación de la red de datos del buque y la instalación de un centro de monitoreo que les permita administrar la información generada en el buque.

Este requerimiento tiene inmerso el chequeo y verificación de los activos que hacen parte de la red de datos ya que es posible que la lentitud que se está generando sea causa de temas de seguridad de la red.

5.2 MARCO TEÓRICO

En Colombia, la Autoridad Marítima hace parte del Ministerio de Defensa Nacional, aunque los buques oceanográficos no hagan parte de la flota de guerra, si hace parte de la fuerza naval, de esta manera se convierten en objetivo militar por tanto susceptible de ataques por parte de grupos criminales, esto conlleva a ataques dentro de los cuales se destacan ataques cibernéticos.

Se le debe sumar a lo anterior, los últimos descubrimientos realizados por buques oceanográficos, como fue el descubrimiento del galeón San José, esta especie naufraga es reclamada por diferentes países, hasta el momento esta información es secreta, en caso de llegar a caer en las personas equivocadas este tesoro encontrado podría ser saqueado, dañado y de esta manera generar más controversia entre las naciones en conflicto por el hallazgo.

La mayor parte de la tecnología a bordo de un buque va dirigida a la protección de su tripulación, de la infraestructura como tal y la obtención de datos, independientemente de cuál sea su especialidad, mas no a proteger la información; las redes informáticas son demasiado básicas, sin protección contra ataques, generan por lo anterior vulnerabilidades que pueden ser aprovechadas para inyectar código maliciosos a sus equipos de cómputo y poder realizar ataques como son robo, alteración y daño a la información, modificación al software de navegación ocasionando encallamientos, daños e incluso hundimientos, en términos generales desastres marítimos[1]

Es evidente que conforme avanza la tecnología, los medios y métodos de comunicación e interacción, también se incrementa el deseo o necesidad de personas, entidades, grupos, entre otros, por atacar las redes de datos, lograr penetrar sus sistemas de información y realizar el robo, daño, alteración, vigilancia de la información de la red atacada. Los ataques a redes informáticas se logran en gran parte por las vulnerabilidades de la misma red y la falta de concienciación en lo que respecta a la seguridad informática por parte de los directores o gerentes, del personal del área de informática y demás funcionarios que componen dicha organización o empresa.

También se puede observar como en muchas empresas no se le da importancia adecuada a la seguridad informática, ya que ven este tema como un gasto y no como una inversión, otro componente que perjudica la seguridad informática es la falta de interés de los funcionarios que componen la empresa y que no tienen continuidad en la misma, la rotación genera desprendimiento y poco interés en temas de seguridad por parte de estos funcionarios. A continuación se describen algunos aspectos relacionados con el proyecto.

---

[1] GOBIERNO DE ESPAÑA – MINISTERIO DE DEFENSA. Revista General de Marina 2015. P. 111 – 112. Disponible en http://publicaciones.defensa.gob.es/pprevistas/dfa2a36b-fb63-65ab-9bdd-ff0000451707/index.html#/112/

5.2.1 Seguridad Informática. Es la disciplina que se encarga del diseño de normas, métodos, técnicas, procedimientos dirigidos a establecer condiciones de seguridad óptimas para el tratamiento de datos en un sistema informático.

Va dirigida al aseguramiento de los activos tecnológicos de una organización, para que estos sean utilizados de la manera correcta y por el personal acreditado para ello.

5.2.2 Principios de Seguridad Informática. La seguridad informática tiene sus bases en tres pilares fundamentales, los cuales se deben cumplir en cualquier sistema informático:

Confidencialidad: Este pilar hace referencia a la privacidad de la información, la seguridad informática debe proteger un sistema informático de acceso a la información por parte de personal o programas no autorizados.

Integridad: Este pilar hace referencia a la veracidad y validez de los datos almacenados o guardados en un sistema informático.

Disponibilidad: Este pilar hace referencia a las condiciones óptimas que deben estar establecidas para que los datos y/o la información se puedan, consultar, verificar, se pueda acceder a la misma en el momento que sea requerido y por personal autorizado.

5.2.3 Red de datos. Es un conjunto de elementos que hacen parte de un parque computacional como con (ordenadores, servidores, impresoras, scanner, etc) los cuales cuentan son su respectivo software, estos elementos se comunican entre sí o con otros equipos de otras redes, a través de unos elementos activos como son (switch, router, Modem, etc) utilizando un utilizando elementos físicos y/o lógicos para transmitir o compartir información.

5.2.4 Vulnerabilidad. Una vulnerabilidad en términos de seguridad informática hace referencia a la debilidad o fallos en cuanto a protección que puede tener un sistema informático. Estas vulnerabilidades pueden permitir que una red de datos o un sistema informático sean penetrados en caso de la ocurrencia de un ataque informático.

5.2.5 Ataques informáticos. Un ataque informático es una acción intencionada o no, mediante la cual se accede a un sistema informático o red sin autorización alguna, este ataque se puede llevar a cabo por parte de personas con grandes conocimientos en informática e incluso con conocimientos básicos, y que buscan causar algún tipo de daño como puede ser el robo, copia, daño, alteración, borrado de información importante para el propietario de la misma.

5.3 MARCO CONCEPTUAL

Ataque Cibernético: Un ataque cibernético consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización. Un ataque cibernético es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etc.).

Pentesting: Es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas. Es una rama de estudio relativamente reciente y en auge (sobrevenido por los importantes ataques y filtraciones sufridos por varias empresas importantes los últimos años).[2]

Software: Un software de computadora está compuesto por una secuencia de instrucciones, que es interpretada y ejecutada por un procesador o por una máquina virtual. En un software funcional, esa secuencia sigue estándares específicos que resultan en un determinado comportamiento.[3]

Look@LAN Network Monitor: Es una aplicación que permite monitorizar las redes de datos. Este software permite controlar todos los nodos de comunicación y realizar test de rendimiento a al sistema operativo, Además advierte mediante alarmas de los posibles cambios que pudiera sufrir la red a través de sus nodos de conexión.[4]

PRTG Network Monitor: Es una aplicación que permite la monitorización que combina la competencia profesional de la compañia de monitorización de redes Paessler con una completa serie de características de monitorización, con una interfaz intuitiva y fácil de usar y tecnología de última generación, adecuado para redes de cualquier tamaño.

PRTG asegura la disponibilidad y mide el tráfico y el uso de los componentes de red. Reduce costos evitando interrupciones, optimizando las conexiones, la carga y calidad, ahorrando tiempo y controlando los Acuerdos de Nivel de Servicio (SLAs).[5]

Nmap: (Network Mapper) es una fuente libre y abierto (licencia de servicios públicos) para la detección de redes y auditoría de seguridad. Muchos sistemas y administradores de red también les resulta útil para tareas tales como inventario de la red, los horarios de actualización de servicio de gestión, monitoreo y anfitrión o un tiempo de servicio. Nmap utiliza paquetes IP en nuevas formas de determinar qué servicios están disponibles en la red de ordenadores, qué servicios (nombre de la aplicación y la versión) los anfitriones están ofreciendo, lo que los sistemas operativos (y versiones del sistema operativo) que se están ejecutando, qué tipo de filtros de paquetes / cortafuegos están en uso, y otras características de docenas. Fue diseñado para escanear rápidamente grandes redes, pero funciona bien contra el anfitrión individuales. Nmap se ejecuta en todos los principales sistemas operativos de los ordenadores, y paquetes binarios oficiales están disponibles para Linux, Windows y Mac OS X. Además de los clásicos de línea de comandos de Nmap ejecutable, la suite Nmap incluye un visor de interfaz gráfica de usuario avanzada y resultados (Zenmap), una transferencia de datos flexible, la redirección, y herramienta de depuración (Ncat), una utilidad para la comparación de los resultados del análisis (Ndiff), y una herramienta de análisis de generación de paquetes y la respuesta (Nping).[6]

---

[2] ESAU. A. 2015. Que es el Pentesting. Disponible en https://openwebinars.net/que-es-el-pentesting/

[3] INFORMATICAHOY. 2012. Que es Hardware y Software. Disponible en http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-Hardware-y-Software.php

[4] WAXOO. Look@LAN Network Monitor. Disponible en http://looklan-network-monitor.waxoo.com/

[5] PAESSLER. "PRTG: Instalado en segundos. Configurado en minutos. Protege redes por años.". Disponible en https://www.es.paessler.com/prtg

[6] NMAP. NMAP. Disponible en https://nmap.org/

GFI LanGuard: es una aplicación que permite escanear la seguridad de la red, permite analizar la red y puertos para detectar, evaluar y corregir vulnerabilidades de seguridad con el mínimo esfuerzo administrativo, permite de esta manera realizar auditorías de red. Esta herramienta permite realizar inventario, gestión de cambios, análisis de riesgo y probar el cumplimiento. GFI LanGuard proporciona una completa imagen de su configuración de red y le ayuda a mantener seguro y en conformidad el estado de la red.[7]

Nessus: Es un programa de software modular para la realización de análisis probabilístico de los componentes estructurales / mecánicas y sistemas. Combina el estado de la técnica de algoritmos probabilísticos con fines generales métodos de análisis numérico para calcular la respuesta probabilístico y la fiabilidad de los sistemas de ingeniería. Las variaciones en la carga, las propiedades del material, geometría, condiciones de contorno, y las condiciones iniciales pueden ser simuladas. NESSUS fue desarrollado inicialmente por SwRI para la NASA para llevar a cabo el análisis probabilístico del transbordador espacial componentes principales del motor. SwRI continúa para desarrollar y aplicar NESSUS a una amplia gama de problemas, incluyendo estructuras aeroespaciales, las estructuras de automoción, la biomecánica , motores de turbina de gas, geomecánica, envases de residuos nucleares, estructuras marítimas, ductos y rotordynamics. Para lograr esto, los códigos se han interconectado con muchos de terceros conocido y programas de análisis deterministas comerciales.[8]

5.4 MARCO LEGAL

5.4.1 Ley 1273 de 2009. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

---

[7] Auditoria y Seguridad Informática. GFI LanGuard. Disponible en http://www.auditoria.com.mx/GFI-LanGuard

[8] TENABLE NETWORK SECURITY. Nessus. Disponible en www.nessus.org

Esta Ley de la Republica de Colombia tipifica los delitos informáticos y establece penas para quienes los cometan, esta ley es una herramienta fundamental para que todas las personas, empresas u organizaciones en el territorio colombiano se protejan jurídicamente y además para evitar la comisión de uno de esos delitos informáticos.

Los artículos que presenta esta Ley:

Capítulo I

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269H: Circunstancias de agravación punitiva.

Capitulo II

- Artículo 269I: Hurto por medios informáticos y semejantes.
- Artículo 269J: Transferencia no consentida de activos.[9]

5.4.2 Documento Conpes 3701. El documento Conpes 3701 de 2011, trata sobre los "LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA".

Este documentos está enfocado al desarrollo de una estrategia nacional permita a través de procedimientos contrarrestar las amenazas informáticas que afectan significativamente al país.[10]

---

[9] CONGRESO DE LA REPUBLICA DE COLOMBIA. 2009. Ley 1273 de 2009. Disponible en http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

[10] CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL – REPUBLICA DE COLOMBIA. 2011. Documento CONPES 3701. Disponible en http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

5.4.3 Norma Técnica Colombiana NTC 5254. "GESTIÓN DE RIESGO" Este documento es una guía genérica para el establecimiento e implementación del proceso de administración de riesgos involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos.[11]

---

[11] ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación). 2006. Documento Norma Técnica Colombiana NTC 5254. Disponible en http://www.corponor.gov.co/NORMATIVIDAD/NORMA%20TECNICA/Norma%20T%E9cnica%20NTC%205254.pdf

6. DISEÑO METODOLÓGICO

El trabajo aplicado se va a desarrollar a través de un proceso de:

- Recolección de información:

1. Levantamiento de información de elementos de la red LAN:

2. Tipos de conexiones desde y hacia la red LAN.

3. Usuarios que interactúan con la red LAN, modalidad, incluye configuración.

- Planificación:

De acuerdo a la información obtenida se procederá a planificar el procedimiento que se deba o pueda realizar.

- Ejecución:

Se llevaran a cabo las siguientes tareas:

1. Revisión de antivirus, malware y otros métodos de defensa, donde se pueda identificar su efectividad, actualización.

2. Revisión de puertos abiertos, privilegios que conceda la configuración de la máquina.

3. Aplicación de Pentesting a la Red LAN, utilizando herramientas importantes como Nmap, GFI LanGuard 2015, PRTG Network Monitor, entre otras que puedan ser necesarias y útiles para la investigación.

- Análisis:

Una vez se haya procedido a levantar información, se haya planificado y se hayan realizado las tareas propuestas se procederá a realizar un análisis de los resultados obtenidos con el fin de identificar posibles vulnerabilidades y debilidades que puedan tener en la red LAN.

- Resultados:

Una vez realizado el análisis se podrán obtener unos resultados los cuales servirán de base para presentar una propuesta de soluciones que se puedan llevar a cabo.

6.1 CLASE DE INVESTIGACIÓN

Proyecto aplicado.

6.2 ÁREA DE CONOCIMIENTO GENERAL Y ESPECÍFICA

• **Área del Conocimiento:** Seguridad en Redes

• **Área Específica***:* Pentesting en redes LAN y WLAN

6.3 INVESTIGADORES Y/O COLABORADORES

AYDEE MERCEDES VIVER RAMIREZ

6.4 PRODUCTOS A ENTREGAR

Documento donde se expongan las herramientas de pentesting aplicadas a la red LAN del buque oceanográfico A.R LIBERTAD con el fin de identificar vulnerabilidades de seguridad, procedimientos realizados, análisis de resultados obtenidos con las herramientas de pentesting ejecutadas, recomendaciones y propuesta de controles a implementar con el fin de mejorar la seguridad de la red.

6.5 ALCANCES DEL PROYECTO O DELIMITACIÓN

Aplicación de herramientas de pentesting a la red LAN del Buque oceanográfico A.R LIBERTAD perteneciente a la Autoridad Marítima Colombiana.

6.6 POBLACIÓN

La población seleccionada para esta investigación es la red LAN del Buque oceanográfico A.R LIBERTAD perteneciente a la Autoridad Marítima Colombiana.

6.7 MUESTRA

Teniendo en cuenta que se toma como Población la red LAN del Buque Oceanográfico A.R LIBERTAD perteneciente a la Autoridad Marítima Colombiana, se determina como muestra para la aplicación de las pruebas de Pentesting los equipos de cómputo asignados para el almacenamiento de la información obtenida en los trabajos de campo y levantamientos batimétricos, estos equipos de cómputo son:

Tabla 1. Muestra seleccionada de la red LAN del buque oceanográfico A.R LIBERTAD

ÁREA O SECCIÓN DE ASIGNACION DE EQUIPO	**FUNCION DEL EQUIPO SELECCIONADO**
Área de Operaciones	Levantamiento de Información 1
Área de Operaciones	Levantamiento de Información 2
Área de Operaciones	Levantamiento de Información 3
Área de Oceanografía	Oceanografía

Fuente: El autor.

7. RECURSOS DISPONIBLES

7.1 RECURSO HUMANO

El proyecto lo llevara a cabo en su totalidad la Ingeniera en informática y estudiante de la especialización en seguridad informática Aydee Mercedes Viver Ramírez.

7.2 RECURSO FÍSICO Y FINANCIERO

En la siguiente tabla se describe el recurso físico y financiero que se requiere para llevar a cabo el proyecto, igualmente se ilustra la fuente de financiación.

Tabla 2. Recurso físico y financiero

CANT.	RECURSO FISICO	VALOR	FUENTE DE FINANCIACION
RECURSO TECNOLOGICO			
1	Equipo de cómputo, core i5 tercera generación, 8 gb en RAM, 500 gb en Disco duro	$2.500.000	Aporte de la Alumna
1	Impresora HP LJ 400 PRO	$650.000	Aporte de la Alumna
1	Toner impresora HP LJ 400 PRO	$300.000	Aporte de la Alumna
1	Disco Duro externo de 500 GB	$120.000	Aporte de la Alumna
1	Internet	$1.056.000	Aporte de la Alumna
	SUBTOTAL	**$4.626.000**	
RECURSOS MATERIALES			
1	Papelería	$80.000	Aporte de la Alumna
	SUBTOTAL	**$80.000**	
	TOTAL RECURSO FINANCIERO	**$4.706.000**	

Fuente: El autor.

7.3 RECURSO TÉCNICO

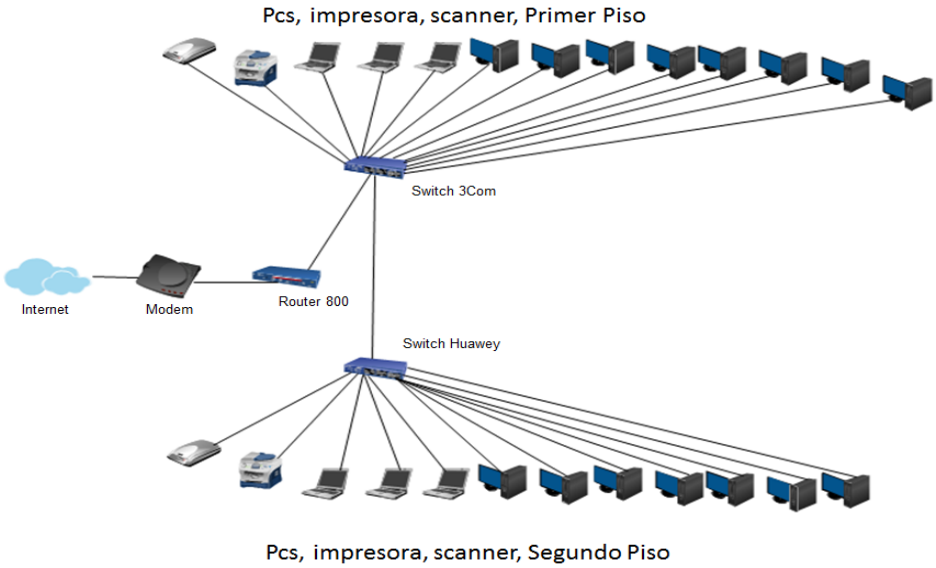
Herramientas de Pentesting: Nmap, Metasploit, GFI LanGuard 2015, PRTG Network Monitor.

8. RESULTADOS Y DISCUSIÓN

8.1 VERIFICACIÓN DE ESTADO DE LA RED LAN DEL BUQUE OCEANOGRÁFICO A.R LIBERTAD PARA REALIZAR RECOMENDACIONES EN CUANTO A SEGURIDAD INFORMÁTICA

A continuación se presenta un diagrama de la red de datos del buque oceanográfico A.R LIBERTAD con el fin de tener una mayor comprensión de la dimensión de la misma. En esta se describe como están conectados todos los dispositivos y elementos que hacen parte de la red.

Figura 1. Diagrama de la red de datos del buque oceanográfico A.R. LIBERTAD



Fuente: El autor.

Para el cumplimiento del objetivo de verificación del estado de la red LAN se realizan las siguientes tareas:

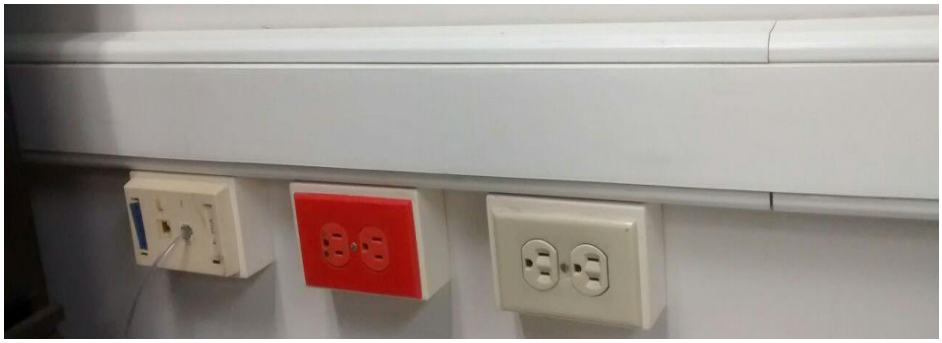
8.1.1 Verificación física de la red. Teniendo en cuenta la importancia del buen estado que debe tener tanto el cableado estructurado de una red como de los

elementos activos que la componen, se realiza una inspección en la cual se tienen en cuenta los siguientes aspectos:

- Estado del cableado estructurado.

  - Tipo de cableado. Cableado UTP categoría 5.
  - La red estructurada la conforman 28 puntos distribuidos en los pisos que componen la superestructura del buque.
  - Planos de la red. Inexistentes.
  - Canaleta.
    - La canaleta utilizada para proteger el cableado en un 80% va entre las paredes del buque por lo tanto solo se verifica el estado del cableado en la canaleta exterior.
    - La canaleta externa es de material plástico.
    - La caja de conexión es tipo universal Panduit.

Figura 2. Canaleta externa de la red de datos del A.R. LIBERTAD



Fuente: El autor.

- Cada punto regulado consta de punto de voz (se utiliza cableado utp pero solo se conectan 2 hilos para telefonía análoga), punto de datos (utp cat 5, 8 hilos), toma dúplex para energía regulada, toma dúplex para energía normal.
- Cableado que llega al Jack RJ45 de cada caja de conexión de puntos de red tienen una curvatura entre 5 y 10 grados lo cual deteriora la calidad de transmisión de datos, no se encuentra bajo la norma IEEE 802.3.

Figura 3. Conexión del cable UTP al Jack de la caja de conexión

Fuente: El autor.

- Los cables UTP cat. 5 y los cables de corriente eléctrica no están separados y organizados como lo indica la norma ANSI EIA/TIA a pesar de que la canaleta tiene una división, esto puede generar interferencias electromagnéticas, ya que este cable no es blindado ni apantallado. Por lo anterior se pueden ver afectados los paquetes de información transmitidos por esta red.

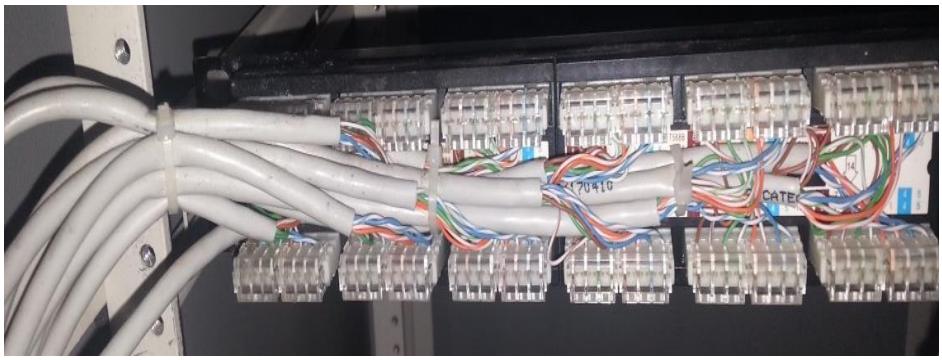
Figura 4. Organización cable UTP y Cable eléctrico en la canaleta externa

Fuente: El autor.

- Verificación tomas eléctricos.
  - En esta revisión se puede observar que los voltajes que se están manejando en la regulada oscilan entre 118V y 130V
  - Energía normal 110 y 115 V

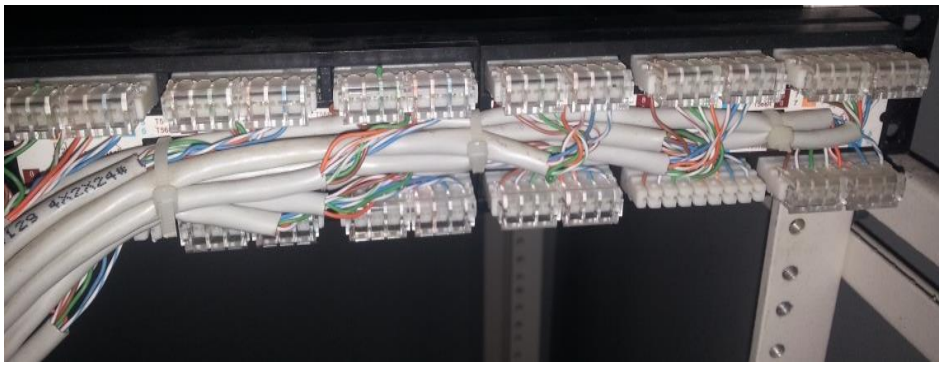
- Se verifica el cableado que llega al patch panel, como se puede observar en las dos siguientes gráficas el cableado no está marcado o identificado.
- La forma de conexión del cableado al patch panel, no se realizó de manera organizada, ordenada y segura, a simple vista en cuanto a conexión no se siguió los estándares ANSI/TIA/EIA-568-B, ANSI/TIA/EIA-569-A, ya que los pares trenzados de diferentes tramas se entrecruzan, además los alambres de cobre están muy expuestos ya que la cubierta fue mal cortada dejando por lo menos 5 o 6 cm de exposición. En caso de requerir un correctivo podría verse afectado un punto de conexión que se encuentre en buen estado.

Figura 5. Organización cable UTP en el Patch panel (lado izquierdo) del rack de comunicaciones



Fuente: El autor.

Figura 6. Organización cable UTP en el Patch panel (lado derecho) del rack de comunicaciones



Fuente: El autor.

❖ Gabinetes de comunicación.

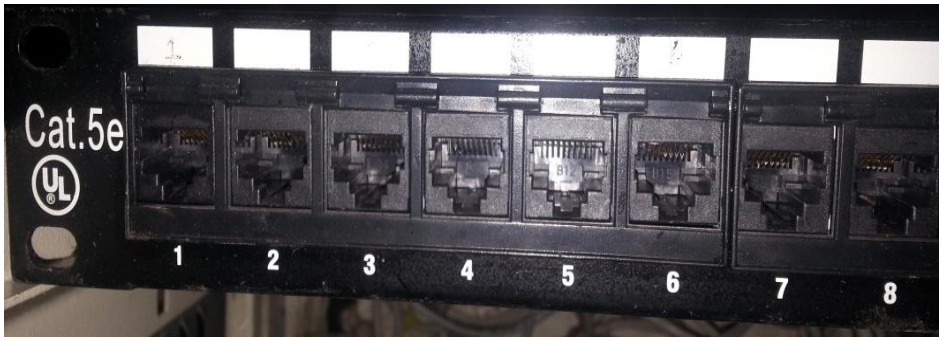
- Marca. Quest
- Estado del Rack de comunicaciones.
  - Presente en su parte externa oxidación.
  - La puerta del rack no cuenta con llave de seguridad.
  - Estado de disipadores de calor. Cuenta con 02 disipadores marca Quest, modelo A12038V1HBL-C, los cuales se encuentran en perfecto estado.
  - Polo a tierra del rack. El rack no se encuentra aterrizado.
  - Verificación del cableado que llega al patch panel. Este cable no tiene la curvatura establecida en la norma, no está marcado, no está conectado de manera correcta.
  - Multiplicador eléctrico. Se encuentra instalado uno de 8 conectores, se encuentra en buen estado
  - Tamaño. El tamaño del rack es de 21U.

- Verificación de elementos instalados en el rack.
  - Switch Huawey S3000, tiene el 80% de los puertos en perfecto estado.
  - Switch 3Com 4200 tiene el 60% de los puertos en mal estado, este switch de acuerdo a información recopilada debe ser reiniciado constatmente ya que se bloquea y los equipos conectados a este switch no puede interactuar en la red.
  - Router Cisco 800 series, se encuentra en perfecto estado.

❖ Patch panel.

- Cuenta con dos patch panel de marca Quest y marca QPCOM, los dos de categoría 5e.
- El patch panel marca Quest no se encuentra debidamente marcado, no se puede identificar a que punto de la red conectará.

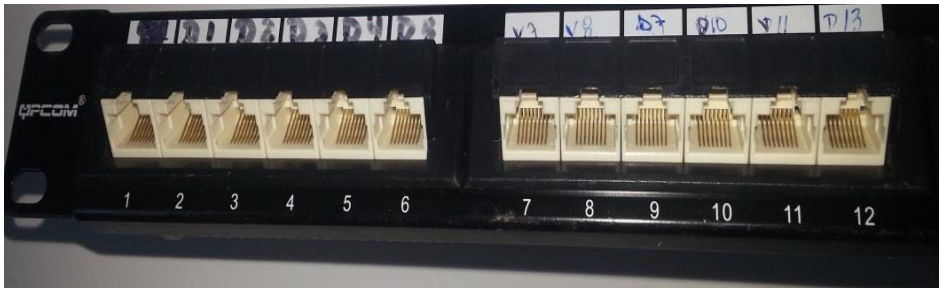
Figura 7. Marcación inexistente en el Patch panel marca Quest



Fuente: El autor.

- El patch panel marca QPCOM tiene una identificación sin embargo los puntos de la canaleta no, lo cual hace complicado saber cuáles puntos de la red conectara, también se puede evidenciar como hace referencia a puntos de voz y datos mezclados.

Figura 8. Marcación en el Patch panel marca QPCOM



Fuente: El autor.

❖ Etiquetado de los cables.

- Marcación de puntos estructurados. Algunos puntos de voz y datos tienen identificación en la canaleta, sin embargo los puntos de energía tanto regulada como normal no se encuentran marcados.
- Las etiquetas utilizadas no son las más estéticas, adecuadas y claras, como se puede ver en la imagen algunas tienen doble etiqueta o marcación (1 cinta de enmascarar, 2 etiqueta en pasta color amarillo indicando si es cable de datos o voz y el número que le

asignaron), sin embargo estas etiquetas no corresponden a los puntos estructurados a que hacen referencia.

Figura 9. Marcación del cableado UTP

Fuente: El autor.

- Data center.

  - Espacio. Teniendo en cuenta que se está hablando de un data center ubicado en un buque con más 30 años de servicio, el espacio asignado es muy reducido es reducido 2 metros de ancho, 2 metros de fondo, 2.1 metros de alto.
  - Aire Acondicionado. Permanente no es un sistema de precisión, es el instalado para toda la embarcación.
  - Iluminación. Cuenta con una sola lámpara la cual está ubicada justo sobre el rack, lo cual impide que la visibilidad en la parte baja del rack sea la adecuada.
  - Estado de limpieza del data center. Por ser un buque militar el aseo es estricto, por tanto el recinto permanece en perfecto estado de limpieza.

- Seguridad Física.

  - Ubicación. El data center se encuentra ubicado al lado izquierdo del camarote del comandante del buque, para acceder a él se debe pasar por el cuarto de mando del buque, este cuarto esta tripulado las 24 horas.
  - Quien ejerce la función de control para acceder al data center es el funcionario de turno designado para prestar vigilancia en el cuarto de mando, sin embargo en caso de una eventualidad este funcionario estará

dando la espalda al data center y no podrá observar quien ingresa o no al mismo.
- Seguridad. No cuenta con cámaras de seguridad, tampoco con sistemas de control de acceso.

- Mantenimiento físico del parque computacional.

  - El mantenimiento que se realiza al parque computacional es preventivo y correctivo cuando se requiera.
  - Se realiza mínimo 2 mantenimientos preventivos al año y es realizado en sitio por personal interno de la institución a la que pertenece el buque, pero que no hace parte de la tripulación del mismo.
  - El mantenimiento correctivo prevé volver el equipo o elemento a su condición normal a todo costo.

- Inventario de equipos activos de la red y parque computacional de la red.

  - Se cuenta con un inventario de equipos los cuales son asignados a un tripulante quien responde ante la entidad por el elemento.
  - Se realiza un chequeo interno cada 6 meses de los elementos y una visita de control interno anual en la cual se hace revisión de la existencia de los mismos.

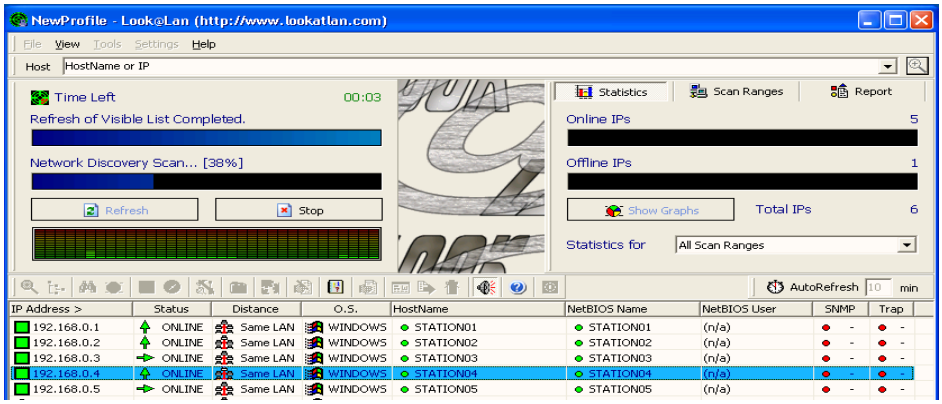
- Garantías sobre equipos activos de la red y parque computacional.

  - En este momento ninguno de los equipos cuenta con garantía por parte del fabricante ya que la misma venció.

8.1.2 Verificación lógica de la red. La verificación lógica se realizó a través de las herramientas de pentesting en el punto 8.1. Aplicación de herramienta de pentesting, para identificar posibles vulnerabilidades sobre la red LAN del buque oceanográfico A.R. LIBERTAD.

Igualmente se realiza a través de la herramienta Look@LAN Network Monitor, monitorización de la red de datos, en la siguiente imagen se puede observar que la comunicación de los nodos se presenta sin novedad, no se registran alarmas por cambios sufridos en la red en el momento de la revisión. Por lo anterior se puede afirmar que la comunicación entre nodos se presenta sin novedad.

Figura 10. Monitorización Red LAN del A.R. LIBERTAD



Fuente: El autor.

8.1.3 Controles y/o medidas establecidas para la seguridad de la red. Una vez realizada la verificación física y lógica de la red LAN del buque oceanográfico A.R. LIBERTAD, se puede determinar que los controles y/o medidas establecidas para la seguridad de la red son nulos.

- No se tienen establecidas para esta red de datos, políticas de seguridad informática.
- No existen restricciones de navegación hacía internet, las restricciones están dadas solo por la ubicación del buque, ya que si se encuentra por fuera del rango de cobertura del proveedor de servicio de internet, el servicio no funcionará,
- La documentación almacenada en los equipos de cómputo está compartida para todos los usuarios sin restricción alguna.
- No existe un Firewall o equipo que haga sus veces.
- No existe un sistema de identificación de intrusos, ni físico, ni lógico.
- No existe un sistema de prevención de intrusos, ni físico, ni lógico.
- Los equipos de cómputo no tienen instalado antivirus, firewall, antimalware, entre otros.
- Los equipos de cómputo no tienen ningún tipo de configuración que pueda brindar seguridad a la máquina y a la red.
- Los usuarios registrados en cada máquina son categoría administrador y no tienen contraseña, por lo cual cualquiera puede ingresar a las máquinas de la red.

8.2 APLICACIÓN DE HERRAMIENTA DE PENTESTING, PARA REALIZAR PRUEBAS DE CAJA BLANCA E IDENTIFICAR LAS VULNERABILIDADES SOBRE LA RED LAN DEL BUQUE OCEANOGRÁFICO A.R LIBERTAD

El primer objetivo planteado indica que se debe realizar la aplicación de Herramientas de Pentesting, para identificar posibles vulnerabilidades sobre la red LAN del buque oceanográfico A.R LIBERTAD.

Para obtener resultados se lleva a cabo un procedimiento por fases así:

- Recolección de Información.
- Planificación.
- Ejecución
- Análisis
- Resultados

8.2.1 Recolección de información. En esta fase se obtiene información correspondiente a todo lo que compete y tiene relación directa con la red de datos del buque, así:

8.2.1.1 Elementos activos de la red. En la siguiente tabla se listan todos los dispositivos que hacen parte de los elementos activos de la red.

Tabla 3. Elementos activos de la red LAN del buque oceanográfico A.R LIBERTAD

TIPO	MARCA	MODELO	CANTIDAD
EQUIPO DE ESCRITORIO	HP	DC5850	15
PORTATIL	LENOVO	THINKPAD	5
PORTATL	TOSHIBA	SATELLITE U505	1
SWITCH	HUAWEY	S3000	1
SWITCH	3COM	4200 26 PORT	1
ROUTER	CISCO	800 SERIES	1

Fuente: El autor.

8.2.1.2 Equipos de cómputo identificados. En la siguiente tabla se listan todos los equipos de cómputo asignados al buque oceanográfico A.R LIBERTAD, e identificados en la red LAN del mismo buque.

Tabla 4. Equipos de cómputo identificados en la red LAN del buque oceanográfico A.R LIBERTAD

ITEM	ÁREA O SECCIÓN DE ASIGNACION DE EQUIPO
1	Comandante del buque
2	Segundo Comandante
3	Primer oficial
4	Segundo oficial
5	Jefe Ingeniero
6	Navegación
7	Operaciones
8	Comunicaciones
9	Levantamiento de Información 1
10	Levantamiento de Información 2
11	Levantamiento de Información 3
12	Batimetría
13	Oceanografía
14	Logística
15	Maquinas
16	Central de almacenamiento
17	Cubierta
18	Radar
19	Administración
20	ECDIS
21	Radar 2

Fuente: El autor.

8.2.1.3 Sistemas operativos identificados.

- Windows XP, este sistema operativo se encuentra instalado en el 71% de los equipos de cómputo que hacen parte de la red.
- Windows 7, este sistema operativo se encuentra instalado en el 29% de los equipos de cómputo que hacen parte de la red.

8.2.1.4 Topología de la red. Topología Estrella.

8.2.1.5 Medio de transmisión. Cableado UTP categoría 5.

8.2.1.6 Conexión a la red. IP estática.

8.2.1.7 Puntos estructurados en la red. 28 puntos estructurados (voz, datos, corriente normal, corriente regulada).

8.2.1.8 Puestos de trabajo instalados actualmente.

- 21 equipos de cómputo.
- 2 impresoras HP LJ 2430
- 2 escáner HP N6350

8.2.1.9 Restricciones establecidas para uso de la red.

- Las restricciones no están dadas por una política de seguridad informática, están dadas por las órdenes del comandante que tenga el buque.
- Las restricciones de navegación hacía internet están dadas solo por la ubicación del buque, ya que si se encuentra por fuera del rango de cobertura del proveedor de servicio de internet, el servicio no funcionará,
- Para una navegación óptima en internet el buque debe estar amarrado en el muelle del puerto al que le asignen tareas de investigación.

8.2.1.10 Privilegios establecidos para uso de la red.

- Carpetas compartidas sin restricciones.
- Navegación sin restricciones.
- Control total de cada equipo al responsable que se le haya asignado.
- Ninguna restricción de uso de los equipos de cómputo de la red.

8.2.1.11 Usuarios que interactúan con la red LAN, modalidad, incluye configuración. Al ser un buque de la Autoridad Marítima Nacional, esta tripulada por personal militar, estas son las personas que tienen acceso a los equipos de la red, el buque tiene una tripulación de 40 marinos, 30 suboficiales y 10 oficiales, sin embargo a las maquinas todos ingresan con un único usuario Administrador.

8.2.2 Planificación. Se realizará trabajo de campo de acuerdo a disponibilidad y autorización del comandante del Buque AR Libertad, la cual dependerá de las operaciones que se estén realizando y la disponibilidad del buque en puerto, esta planificación está enmarcada en el cronograma propuesto.

8.2.3 Ejecución y evidencia de resultados obtenidos con herramientas de pentesting. Se llevan a cabo las siguientes tareas:

8.2.3.1 Herramientas de Pestesting utilizadas.

- NMAP
- GFI LANGUARD 2015
- PRTG NETWORK MONITOR

8.2.3.2 Revisión de antivirus, malware y otros métodos de defensa, donde se pueda identificar su efectividad y actualización. Se realiza revisión de los métodos de defensa existentes o implementadas en los equipos seleccionados en la muestra, en la siguiente se expone la información obtenida.

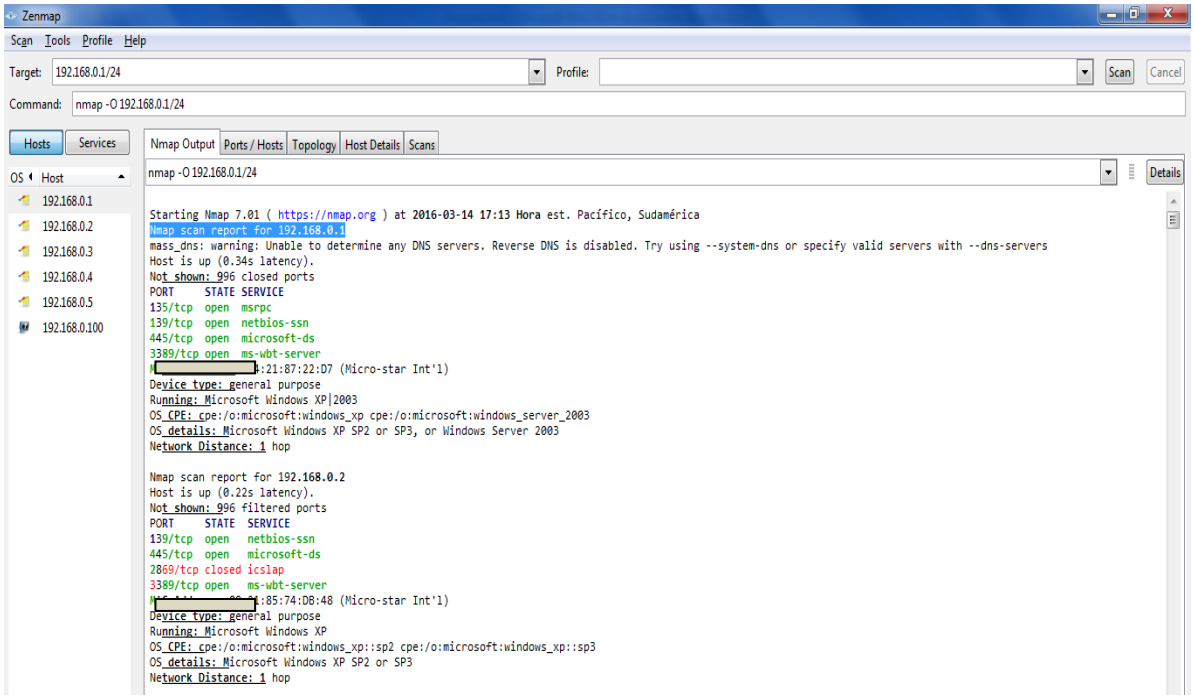
Tabla 5. Métodos de defensa

AREA DE ASIGNACIÓN	EQUIPO DE COMPUTO	IP	ANTIVIRUS	MALWARE	OTROS METODOS DE DEFENSA
NAVEGACIÓN	HP – DC5850	192.168.0.1	NO TIENE	NO TIENE	NO TIENE
ÁREA DE OPERACIONES	HP – DC5850	192.168.0.2	NO TIENE	NO TIENE	NO TIENE
LEVANTAMIENTO DE INFORMACIÓN 1	HP – DC5850	192.168.0.3	AVG - DESACTUALIZADO	NO TIENE	NO TIENE
COMUNICACIONES	HP – DC5850	192.168.0.4	NO TIENE	NO TIENE	NO TIENE
ÁREA DE OCEANOGRAFÍA	LENOVO	192.168.0.100	NO TIENE	NO TIENE	NO TIENE

Fuente: El autor.

8.2.3.3 Revisión de puertos abiertos, privilegios que conceda la configuración de la máquina y evidencia de resultados obtenidos con Herramientas de Pentesting. Se corren herramientas de pentesting a los equipos seleccionados en la muestra, la primera herramienta que se utiliza es NMAP, con esta herramienta se puede obtener información de la configuración de cada máquina, se detallará la información obtenida por ip.

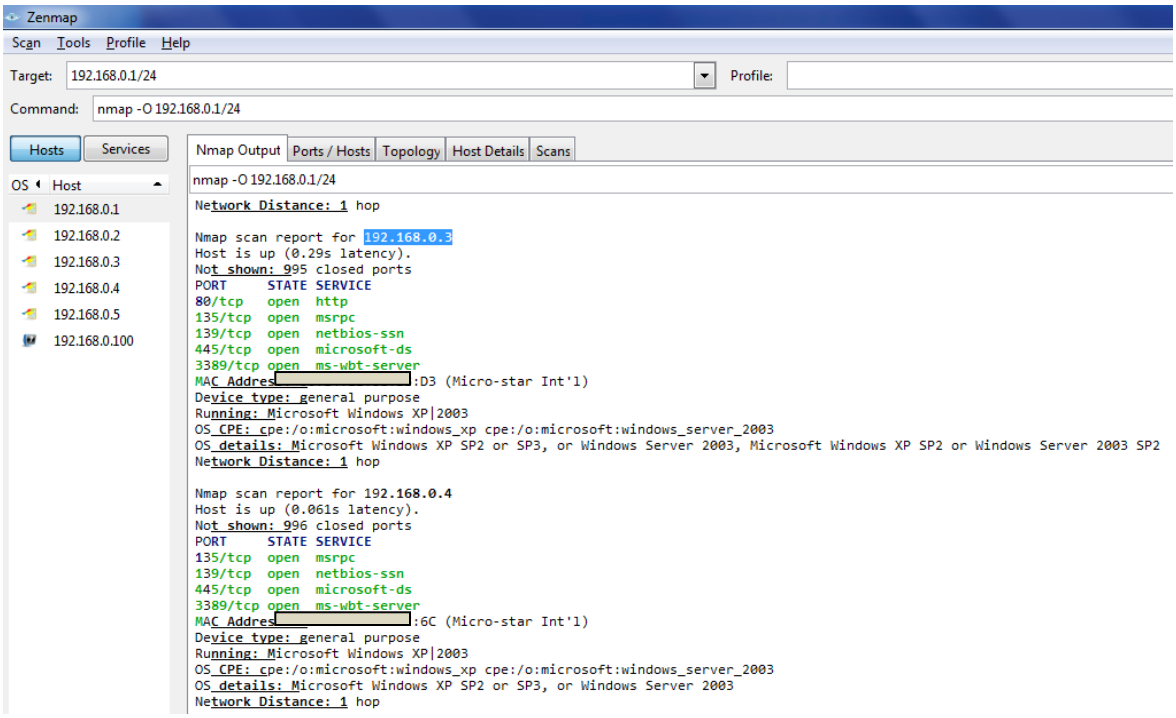
Figura 11. Se identifican los puertos abiertos de los equipos correspondientes a la IP 192.168.0.1 y 192.168.0.2



Fuente: El autor.

En la siguiente figura se puede observar la información obtenida acerca de los puertos abiertos que tienen dos de los equipos de cómputo conectados a la red de datos.

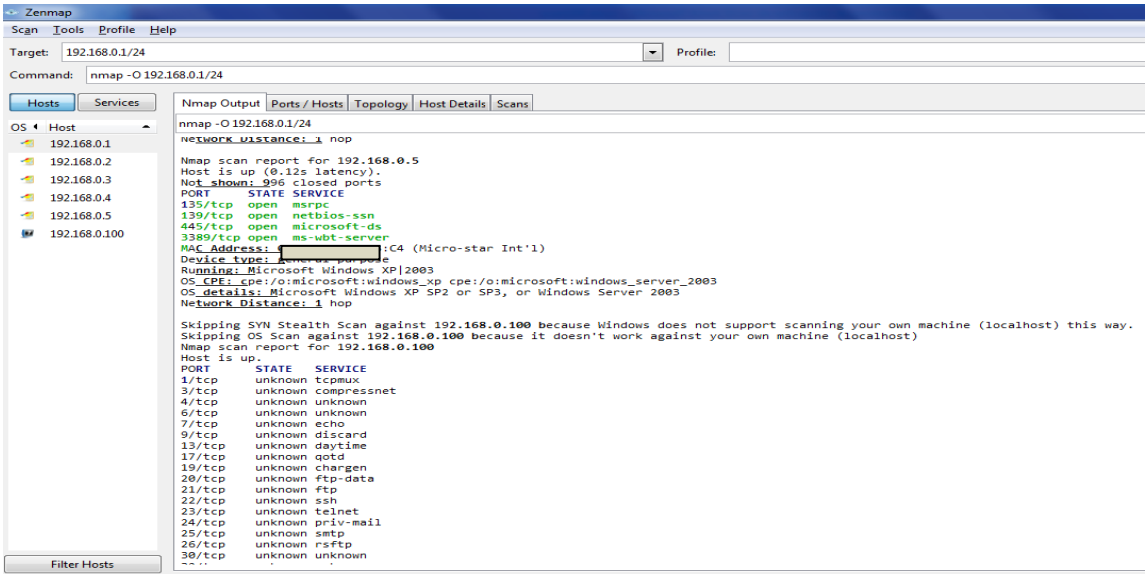
Figura 12. Se identifican los puertos abiertos de los equipos correspondientes a la IP 192.168.0.3 y 192.168.0.4



Fuente: El autor.

En la siguiente figura se puede observar la información obtenida acerca de los puertos abiertos que tienen dos de los equipos de cómputo conectados a la red de datos.

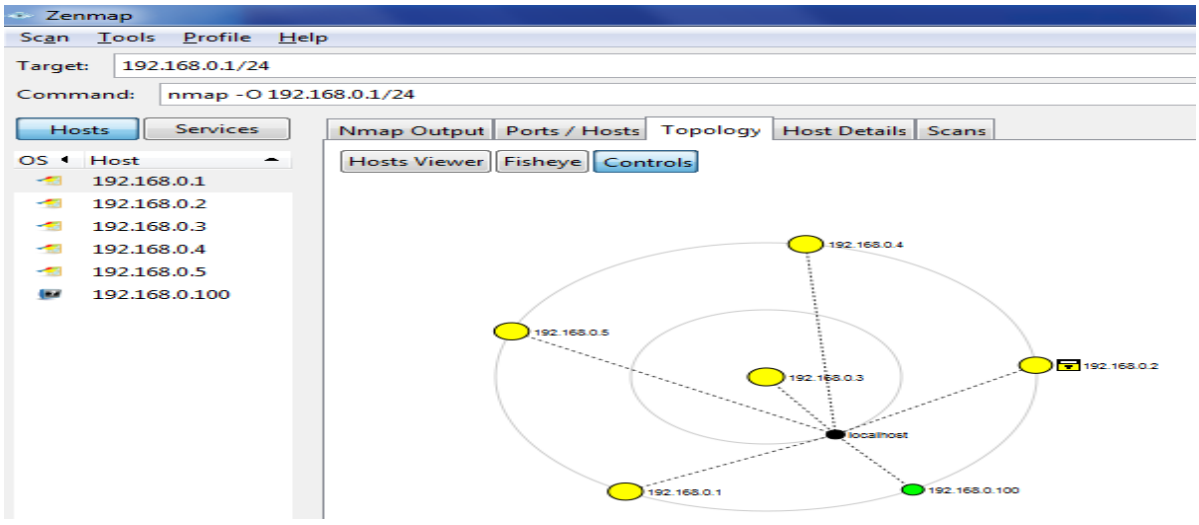
Figura 13. Se identifican los puertos abiertos del equipo correspondientes a la IP 192.168.0.100



Fuente: El autor.

A través de la herramienta NMAP se obtiene gráficamente la topología de la red de datos, se tienen en cuenta solo los equipos seleccionados en la muestra.

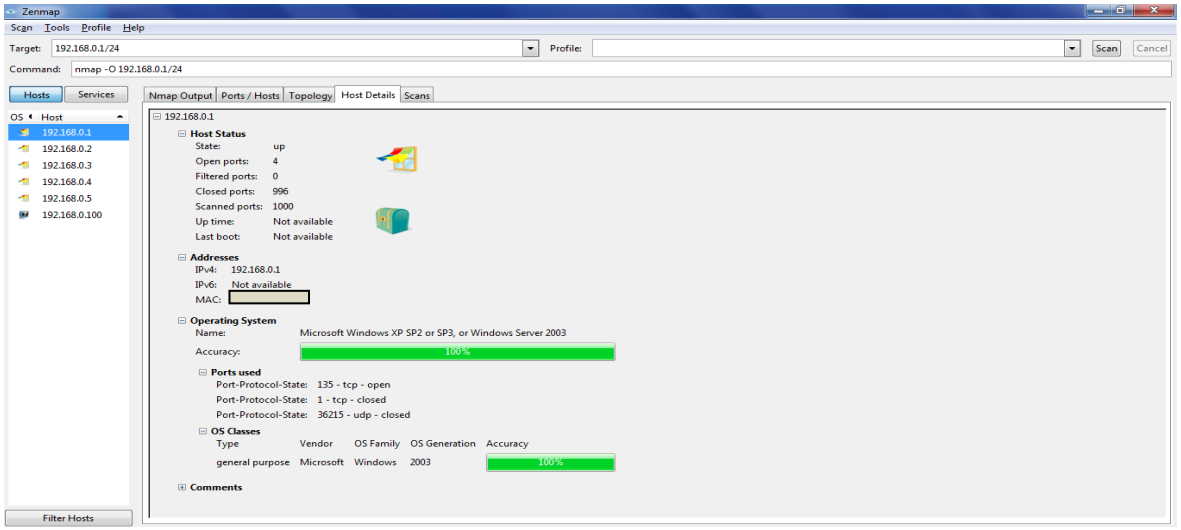
Figura 14. Esquema de la topología de red identificada por Nmap con los equipos que se seleccionados en la de muestra



Fuente: El autor.

Utilizando Nmap se obtiene información detallada de la configuración de cada equipo seleccionado en la muestra, esta información se expone identificando cada equipo por la ip asignada. Esta información se puede detallar en la siguiente figura.

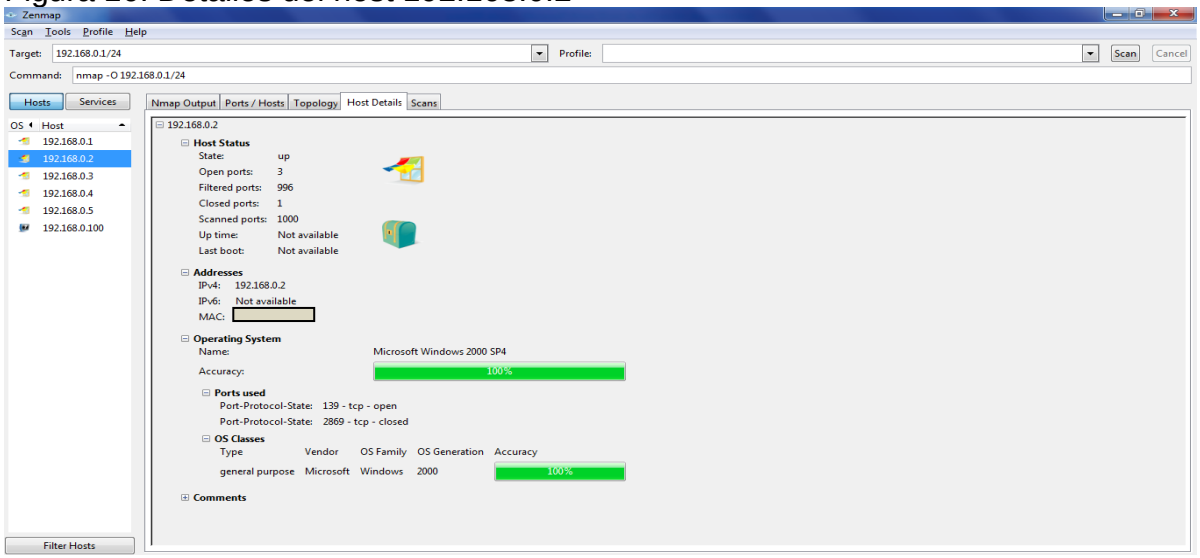
Figura 15. Detalles del host 192.168.0.1



Fuente: El autor.

En la siguiente figura se puede observar la información detallada de la configuración de cada equipo seleccionado en la muestra, esta información se expone identificando cada equipo por la ip asignada.

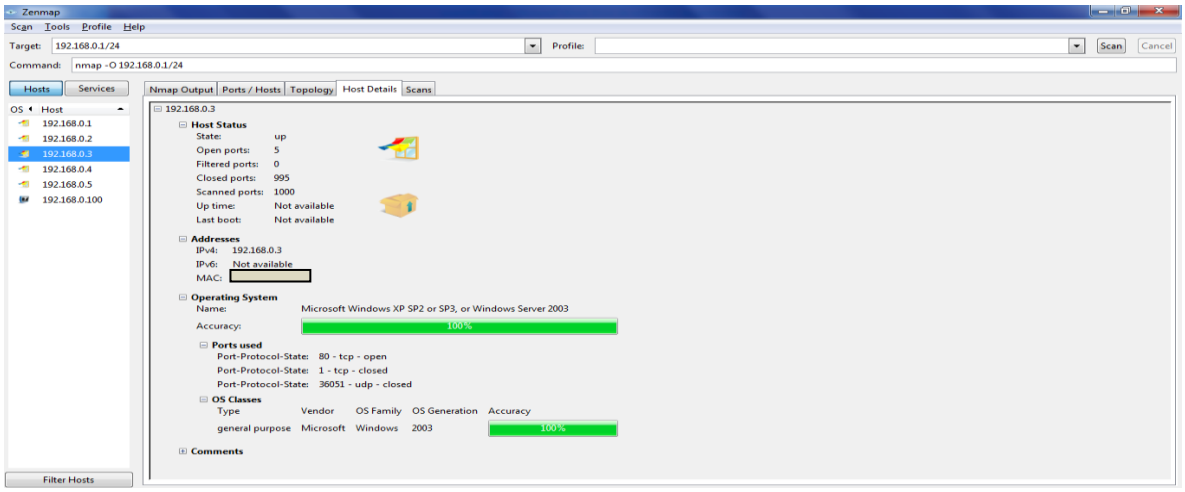
Figura 16. Detalles del host 192.168.0.2



Fuente: El autor.

En la siguiente figura se puede observar la información detallada de la configuración de cada equipo seleccionado en la muestra, esta información se expone identificando cada equipo por la ip asignada.

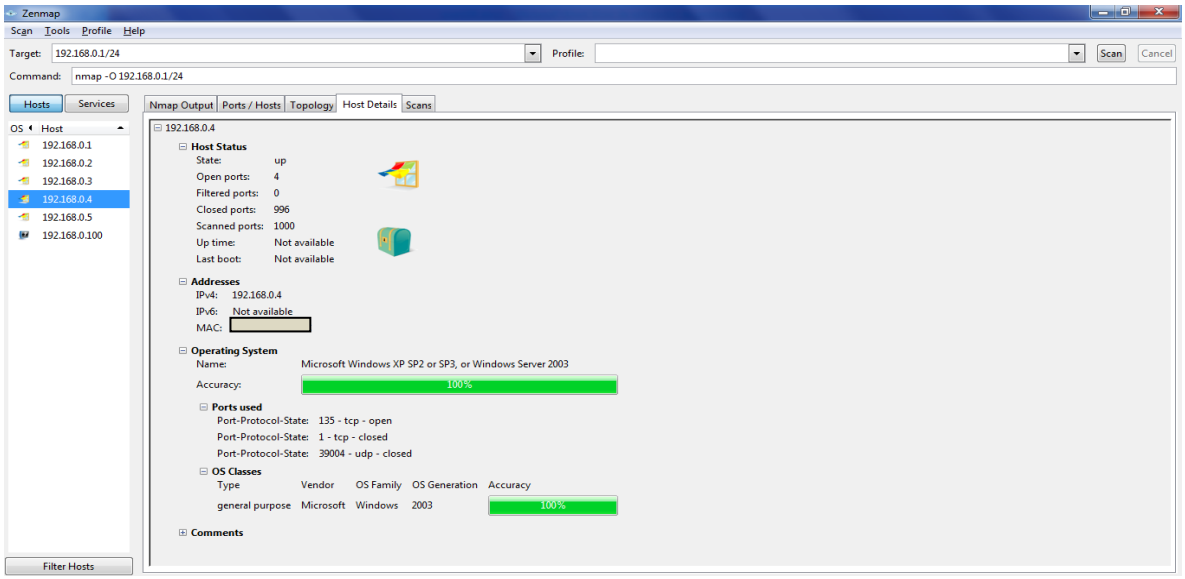
Figura 17. Detalles del host 192.168.0.3



Fuente: El autor.

En la siguiente figura se puede observar la información detallada de la configuración de cada equipo seleccionado en la muestra, esta información se expone identificando cada equipo por la ip asignada.

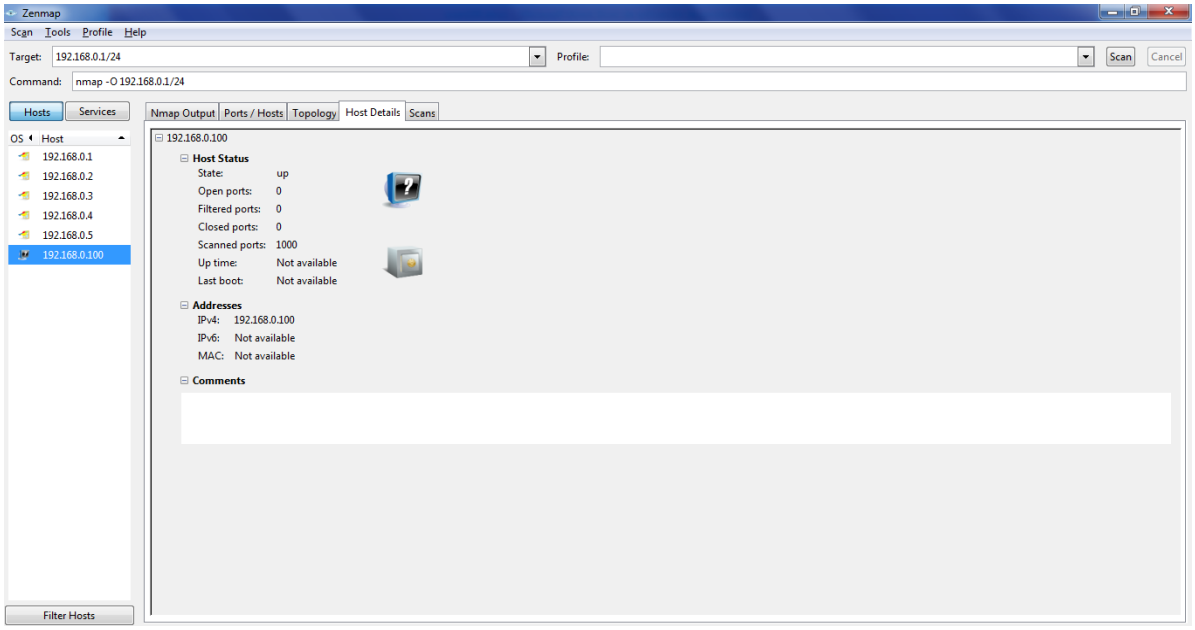
Figura 18. Detalles del host 192.168.0.4



Fuente: El autor.

En la siguiente figura se puede observar la información detallada de la configuración de cada equipo seleccionado en la muestra, esta información se expone identificando cada equipo por la ip asignada.

Figura 19. Detalles del host 192.168.0.100

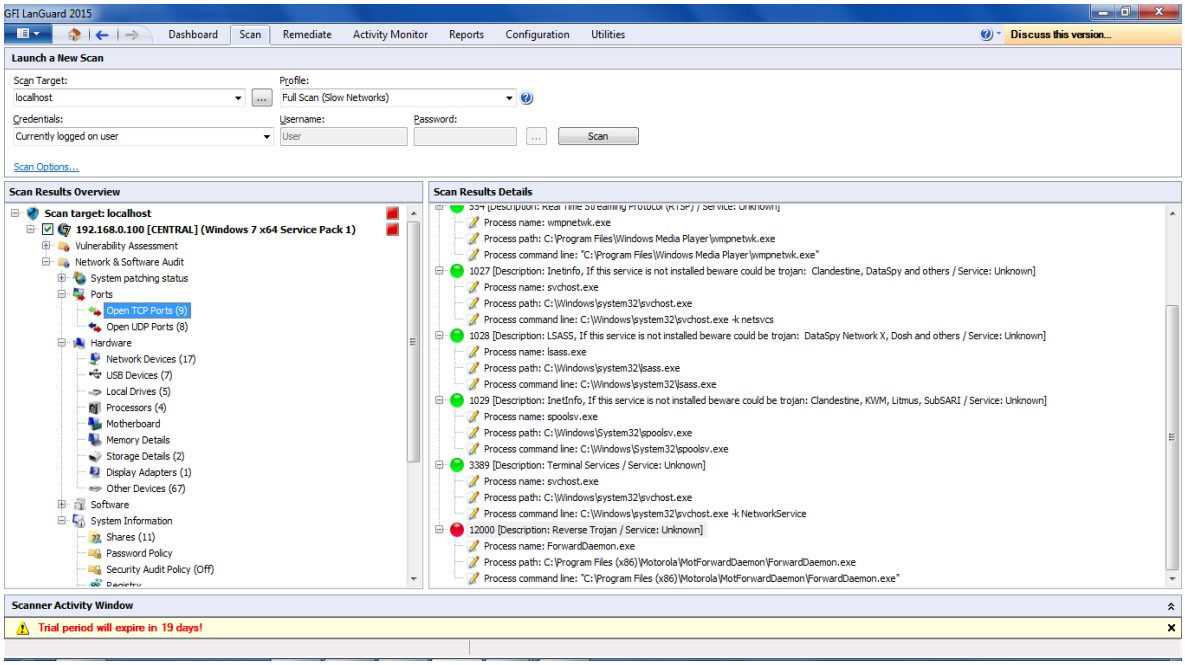


Fuente: El autor.

8.2.3.4 Aplicación de la herramienta GFI LanGuard 2015 para identificar posibles vulnerabilidades. Teniendo en cuenta la necesidad de detectar las vulnerabilidades presentes en la red del buque oceanográfico A.R. LIBERTAD, se utilizó la herramienta GFI LanGuard 2015, se obtienen los siguientes resultados:

En la siguiente figura se puede observar que la herramienta GFI LanGuard 2015 complementa los resultados obtenidos con NMAP, se obtiene el listado de puertos abiertos y la descripción de cada servicio, lo relevante en esta primera observación es que se puede identificar la primera vulnerabilidad, la existencia de un troyano.

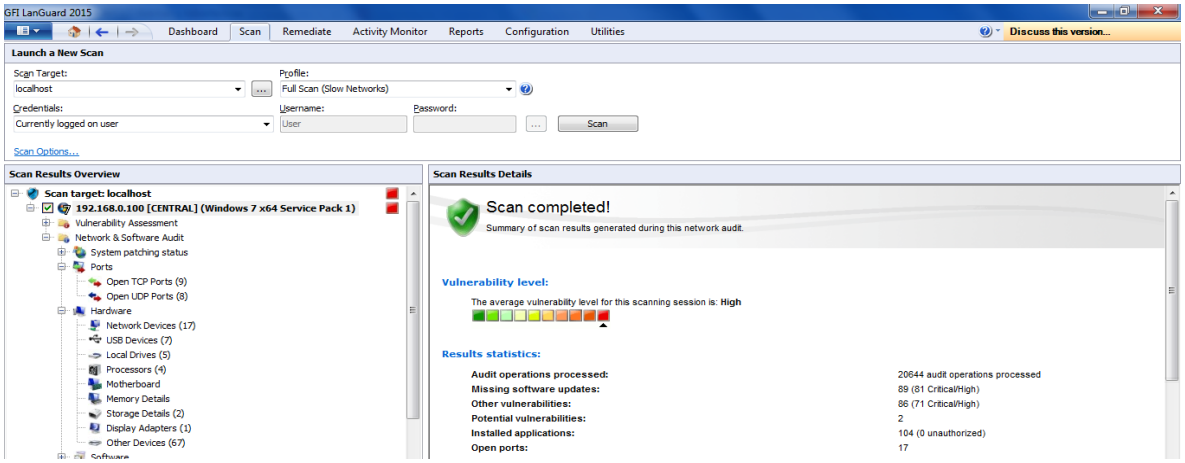
Figura 20. Identificación de puertos abiertos host 192.168.0.100



Fuente: El autor.

En la siguiente figura se puede observar de manera más completa el nivel de vulnerabilidad que tienen los quipos de la red, al no contar con ningún sistema de protección el nivel de vulnerabilidad de las maquinas es el más alto que es de 10.

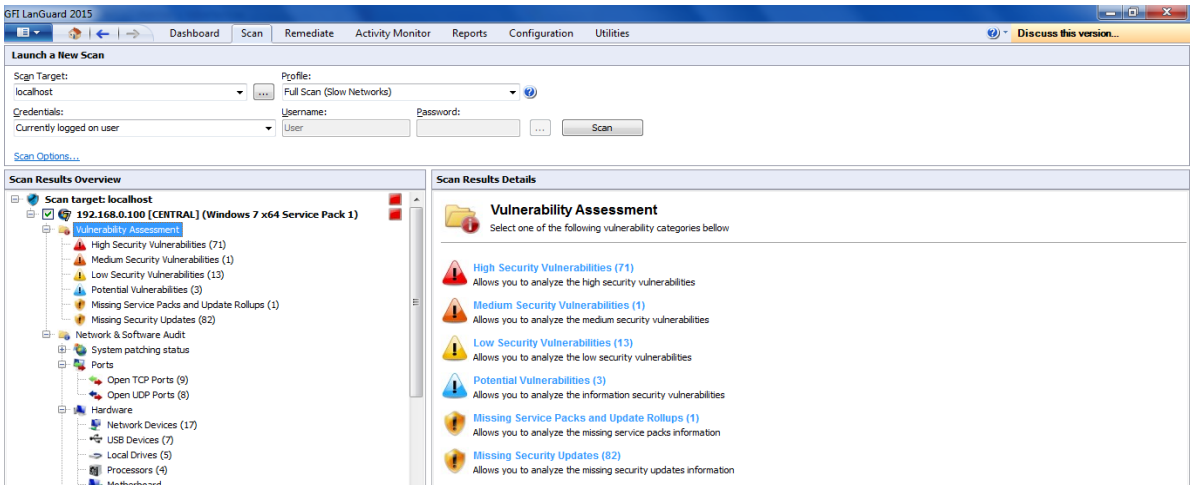
Figura 21. Nivel de vulnerabilidad de la red



Fuente: El autor.

En la siguiente figura la herramienta GFI LanGuard 2015 presenta la evaluación de las vulnerabilidades encontradas por categorías, como se puede observar el nivel de vulnerabilidad es demasiado alto.

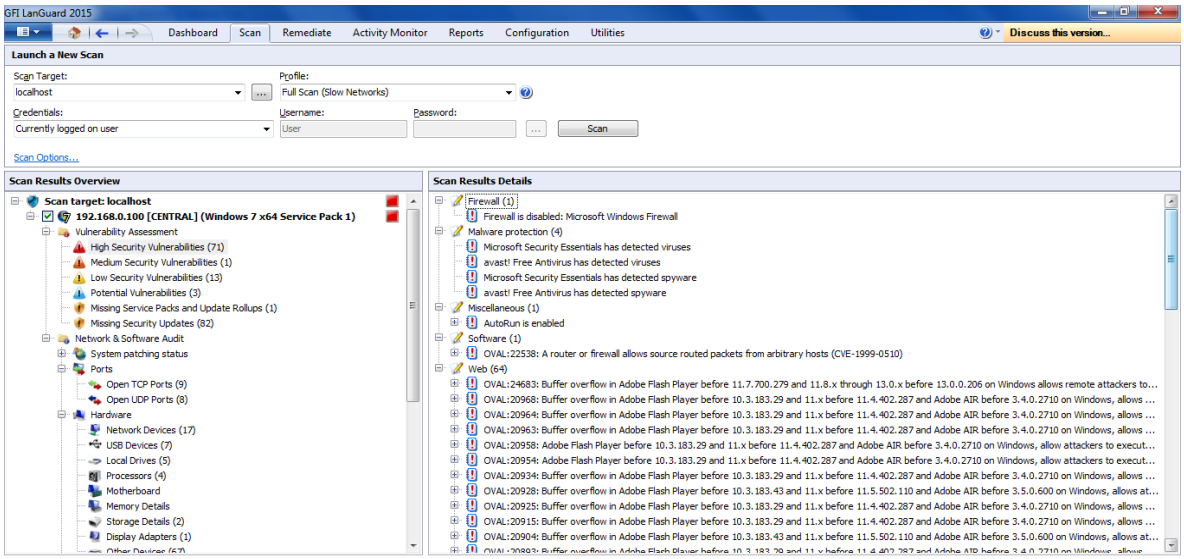
Figura 22. Evaluación de vulnerabilidades encontradas en los equipos de la red



Fuente: El autor.

En la siguiente figura se puede observar de manera mucho más detallada cada vulnerabilidad presente en los equipos de la red, se puede evidenciar la ausencia de un Firewall, la presencia de virus y spyware y las fallas en la configuración de seguridad de los equipos de la red.

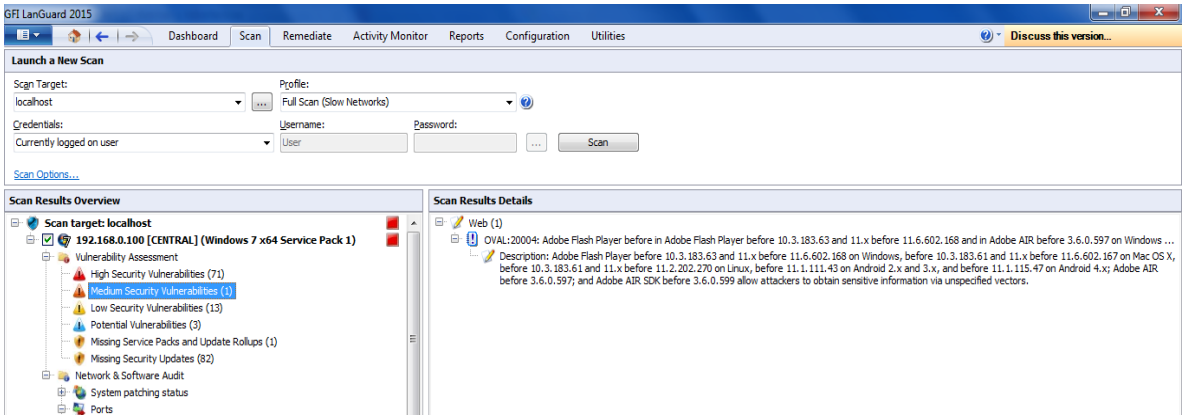
Figura 23. Informe de vulnerabilidades por categorías



Fuente: El autor.

En la siguiente figura se puede evidenciar la vulnerabilidad de categoría media que arroja la herramienta GFI LanGuard 2015. En los equipos de la red están presentes vulnerabilidades en la configuración que pueden permitir a un atacante obtener información sensible a través de vectores no especificados.

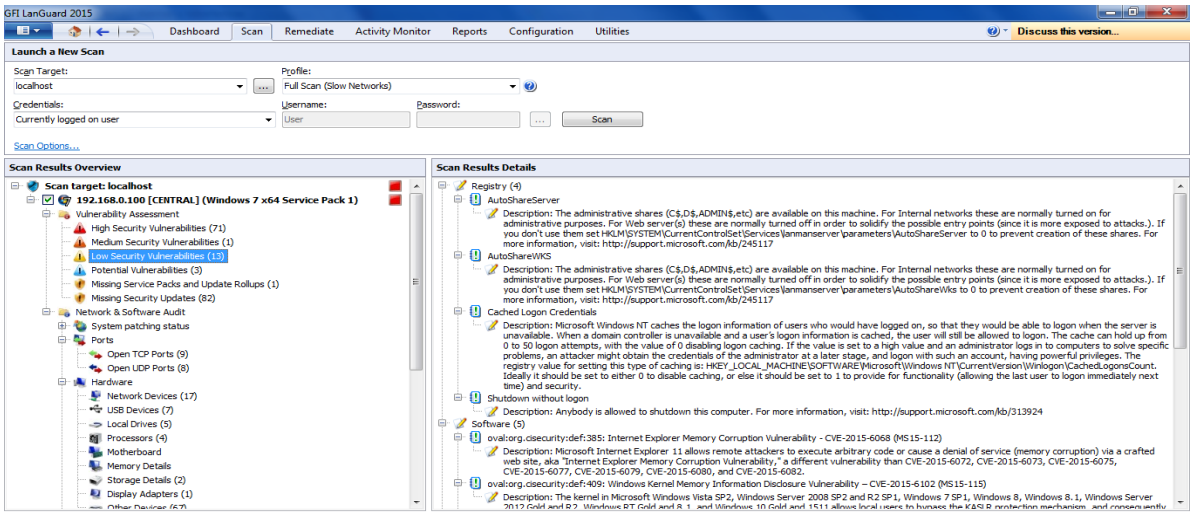
Figura 24. Informe de vulnerabilidades categoría media



Fuente: El autor.

En la siguiente figura se puede evidenciar la vulnerabilidad de categoría baja que arroja la herramienta GFI LanGuard 2015. En los equipos de la red están presentes vulnerabilidades desde el registro y cache de los equipos de cómputo, si bien son vulnerabilidades de categoría baja, estas pueden ser utilizadas para ocasionar un daño a la seguridad de la red.

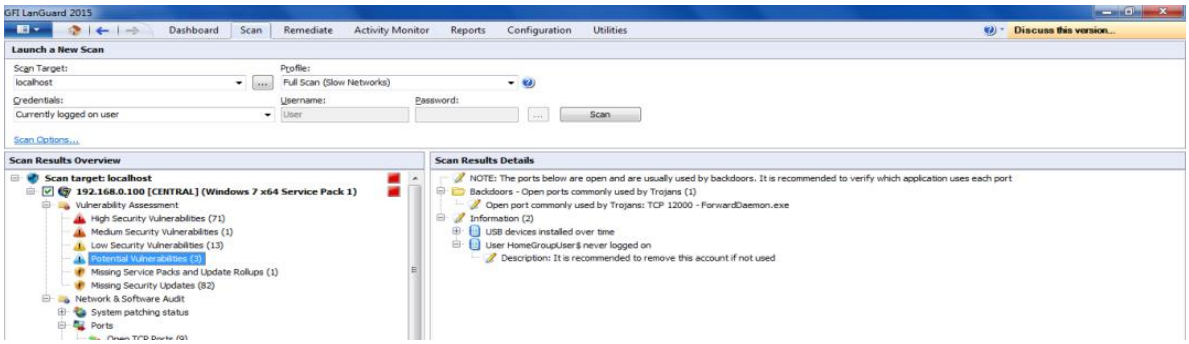
Figura 25. Informe de vulnerabilidades categoría baja



Fuente: El autor.

En la siguiente figura se puede evidenciar las vulnerabilidades potenciales del sistema, estas evidencias pueden permitir utilizar puertos por troyanos que ocasionen daño a la seguridad de la red.

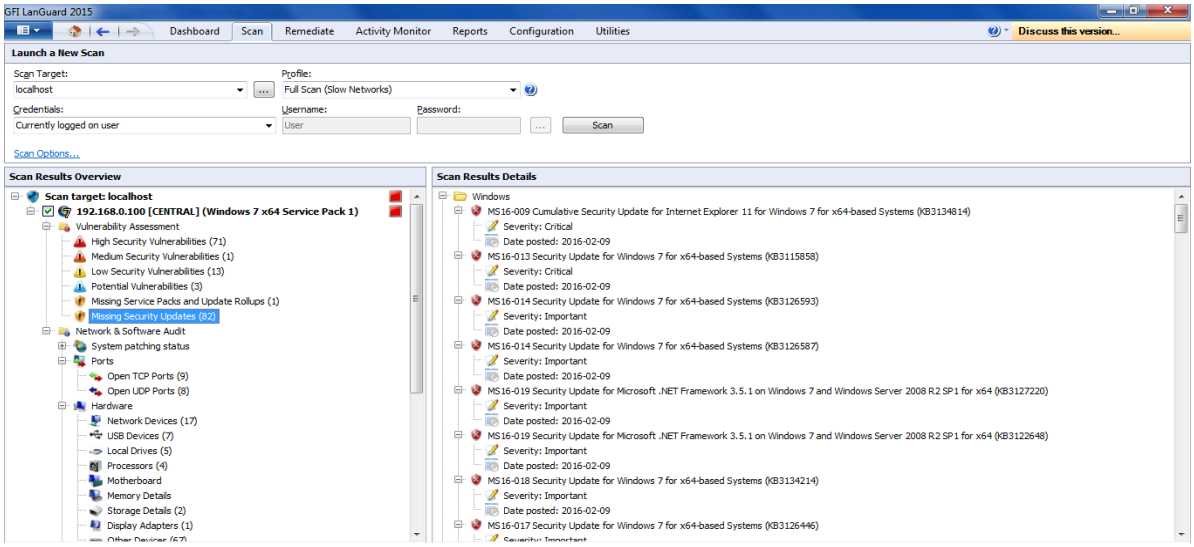
Figura 26. Informe de vulnerabilidades potenciales



Fuente: El autor.

En la siguiente figura se puede evidenciar la falta de actualizaciones de seguridad del sistema operativo.

Figura 27. Informe de vulnerabilidades por falta de actualizaciones del sistema



Fuente: El autor.

8.3 REALIZAR UN ANALISIS COMPLETO Y DETALLADO SOBRE EL ESTADO DE LA RED LAN DEL BUQUE OCEANOGRÁFICO A.R LIBERTAD.

Se realiza un análisis completo y detallado sobre el estado de la red LAN del Buque Oceanográfico A.R LIBERTAD cuya finalidad es presentar recomendaciones basadas en los hallazgos que se realicen; estas recomendaciones estarán enfocadas en acciones o controles que se deben realizar para reducir ataques por vulnerabilidades que se puedan presentar en la red LAN.

8.3.1 Análisis de hallazgos sobre la red LAN del buque oceanográfico A.R LIBERTAD. Con el fin de determinar las vulnerabilidades que pudiese tener la red de datos de AR Libertad, como primera medida se realiza una visita en sitio, en esta visita se realiza el levantamiento del inventario físico de los equipos de la red y los elementos activos de la misma, se pudo evidenciar:

- La red de datos no cuentan con un Sistema de Detección de Intrusos (IDS) ni tipo hardware ni tipo software.
- La red de datos no cuenta con un Sistema de Prevención de Intrusos (IPS), ni tipo hardware, ni tipo software.
- La red de datos no cuenta con un firewall, ni tipo hardware ni tipo software.
- Los equipos de cómputo tienen instalado como sistema operativo:
    - Windows XP, este sistema operativo se encuentra instalado en el 71% de los equipos de cómputo que hacen parte de la red.
    - Windows 7, este sistema operativo se encuentra instalado en el 29% de los equipos de cómputo que hacen parte de la red.

Una vez identificados todos los elementos de la red, y seleccionada la muestra con la cual se iba a trabajar, se corren herramientas de pentesting como son NMAP, GFI LanGuard, PRTG Network Monitor, se identificaron una serie de novedades en la red LAN del buque oceanográfico A.R LIBERTAD de la autoridad colombiana, así:

- En cuanto a métodos de defensa como son antivirus, malware, firewall, IDS, IPS que se deberían tener instaladas y configuradas en los equipos de cómputo, se pudo evidenciar:
    - Solo un equipo de cómputo cuenta con antivirus, el antivirus utilizado es una versión gratuita de AVG, pero este se encuentra desactualizado.
    - A través de la herramienta GFI LanGuard 2015 se identifica la existencia de un troyano identificado con el nombre de (Reverse trojan/service), su alias (BackDoor Reversetrojan) este software

malicioso permite a cualquier hacker el acceso remoto a la maquina o maquinas infectadas para así poder dañar, copiar, eliminar, alterar información almacena en la maquina infectada, igualmente pueden realizar instalación de software no deseado como pueden ser keylogger, troyano LAN.

- En cuanto a los sistemas operativos que se encuentran instalados en los equipos de cómputo se pudo evidenciar que están totalmente desactualizados, tanto el Windows XP, como Windows 7, lo que genera fallas graves en la seguridad de cada equipo desactualizado y en la seguridad de la red.
- Se realiza revisión de puertos abiertos y su configuración, se obtienen la siguiente información:

  - Puerto 135/tcp open msrpc (Este puerto presentan vulnerabilidades descubiertas en las distintas versiones de Windows. Un atacante puede explotar las más severas de ellas, para tomar el control total del equipo afectado, incluyendo la instalación de programas; visualización, cambio o borrado de datos; o crear nuevas cuentas de usuario con todos los privilegios). Los host con Windows XP y que no tengan el service pack 3 instalado y los parches de seguridad publicados por Microsoft, están expuestos a ataques informáticos utilizando código abierto libre y a través de metasploit.
  - Puerto 139/tcp open netbios – ssn. (Este puerto presentan vulnerabilidades descubiertas en las distintas versiones de Windows. Un atacante puede explotar las más severas de ellas, para tomar el control total del equipo afectado, incluyendo la instalación de programas; visualización, cambio o borrado de datos; o crear nuevas cuentas de usuario con todos los privilegios). Los host con Windows XP y que no tengan el service pack 3 instalado y los parches de seguridad publicados por Microsoft, están expuestos a ataques informáticos utilizando código abierto libre y a través de metasploit. Los siguientes troyanos pueden ser utilizados para realizar ataques a través de este puerto: Chode , Hacker fuego , Msinit , Nimda , Opaserv , Qaz.
  - Puerto 445/tcp open Microsoft –ds. (Este puerto presentan vulnerabilidades descubiertas en las distintas versiones de Windows. Un atacante puede explotar las más severas de ellas, para tomar el control total del equipo afectado, incluyendo la instalación de programas; visualización, cambio o borrado de datos; o crear nuevas cuentas de usuario con todos los privilegios). Los host con Windows XP y que no tengan el service pack 3 instalado y los parches de seguridad publicados por Microsoft, están expuestos a ataques informáticos utilizando código abierto libre y a través de metasploit. El troyano Nimba pueden ser utilizados para realizar ataques a través de este puerto.

- Puerto 3389/ tcp open ms-wbt-server. Este puerto presenta vulnerabilidades a ataques de denegación de servicio contra Windows NT Terminal Server, este ataque se puede realizar de manera remota. El atacante provoca que se genere demasiado consumo de memoria a través de múltiples conexiones TCP normales al puerto 3389, lo que permite una denegación de servicio, esta vulnerabilidad está presente en sistemas operativos Windows 7.

- El análisis de vulnerabilidad arrojo como resultado un nivel de vulnerabilidad de 10 sobre 10, este resultado se da debido a la falta de sistemas operativos debidamente actualizados, falta de métodos de protección tanto en la red como en cada una de las maquinas, falta de controles y restricciones hacia los usuarios. Como consecuencia se puede evidenciar:
  - Firewall del sistema operativo deshabilitado.
  - Vulnerabilidades web.
    - Se descubre desbordamiento de búfer en el Adobe Flash Player utilizado por los equipos de cómputo de la red, esto permite que atacantes de manera remota puedan ejecutar código arbitrario a través de vectores no especificados, el impacto de esta vulnerabilidad puede afectar la confidencialidad, integridad, disponibilidad, autenticidad del servicio.
    - Se identifica vulnerabilidad en los equipos con sistema operativo Windows 7, ya que el firewall esta deshabilitado o no se encuentra configurado correctamente, se pudo evidenciar que el "Registro de paquetes perdidos" no tiene la selección de la opción perfil privado.
    - Se identifica vulnerabilidad en los equipos con sistema operativo Windows 7, ya que el firewall esta deshabilitado o no se encuentra configurado correctamente las Conexiones salientes - no tiene la selección de la opción perfil privado.
    - Se identifica vulnerabilidad en los equipos con sistema operativo Windows 7, ya que el firewall esta deshabilitado o no se encuentra configurado correctamente, por ello La ruta del archivo de registro y el nombre del servidor de seguridad de Windows puede ser atacado desde el perfil público.
    - Se identifica vulnerabilidad por desbordamiento de búfer en los equipos de cómputo que tienen instalada la aplicación Movie Maker debido a la falta de métodos de seguridad, en especial la configuración del firewall del sistema operativo nativo.
  - Presencia de virus
  - Presencia de spyware

- Dentro el análisis de vulnerabilidad también se identifican una vulnerabilidad generada luego de conectar en el equipo de cómputo un dispositivo Motorola e instalar el software del fabricante, este activa el Servicio PST que se ejecuta como la cuenta del sistema con amplios privilegios en el equipo local, y actúa como el equipo de la red abre el puerto TCP 12000, este puerto es utilizado como puerta trasera y a través de troyanos realizar ataques a la seguridad.

Posterior a la identificación de vulnerabilidades con herramientas de pentesting, y con el fin de complementar el tema de la seguridad de la red de datos, se realiza la verificación física (en la cual se tiene en cuenta el estado del cableado estructurado de la red LAN y sus elementos activos) se encuentran las siguientes novedades:

Verificación física de la red LAN:

- Al realizar inventario de los activos de la red, se pudo evidenciar que no existen planos de la red estructurada, lo cual dificulta la labor de identificación de novedades sobre el cableado.
- Una vez revisado el cableado de datos que llega al Jack RJ45 de cada caja de conexión de los puntos de la red, se puede observar que este tiene una curvatura entre 5 y 10 grados, esta curvatura puede afectar la calidad de transmisión de datos.
- La red estructurada utiliza canaleta plástica, esta canaleta trae la división para separar el cableado de voz y datos del cableado eléctrico, sin embargo se puede observar que estos cables se encuentran en la misma división de la canaleta, esto puede generar interferencias electromagnéticas, ya que este cable no es blindado ni apantallado. Por lo anterior se pueden ver afectados los paquetes de información transmitidos por esta red.
- Los voltajes de energía que están recibiendo los puntos regulados donde se están conectados los equipos de cómputo de la red están por encima del estándar.
- El cableado estructurado, no se encuentra marcado en ninguno de sus extremos, lo cual dificulta la verificación del mismo y la identificación y corrección de fallas.
- El rack presenta novedades como es la incorrecta marcación del cableado que llega a cada patch panel y la marcación de los patch panel, la conexión no sigue los estándares establecidos a nivel mundial, el rack presenta señales de oxidación, la puerta no cuenta con llave de seguridad y el polo a tierra no está conectado.
- Los dos switch utilizados para la comunicación entre los equipos de la red presentan fallas, el switch de marca 3Com debido a su mal estado genera caídas en el servicio de conexión tanto para los equipos conectados en este

switch como para los demás equipos de cómputo de la red, el switch Huawey presenta varios puertos fuera de servicio.

- La iluminación del data center es muy pobre debido a que se encuentra instalada una sola lámpara y su ubicación es sobre el rack, lo cual impide que la visibilidad en la parte baja del rack sea la adecuada.
- La seguridad del data center recae solamente en el personal de guardia de turno, este sector no tiene cámaras de seguridad en la cual se pueda registrar las actividades que se presenten en este sitio.

En cuanto a los controles y/o medidas de seguridad establecidas para proteger la red de datos se pudo establecer que son nulos, estas son las principales novedades detectadas:

- No se tienen establecidas para esta red políticas de seguridad informática.
- No existen restricciones de navegación hacía internet, están dadas solo por la ubicación del buque, ya que si se encuentra por fuera del rango de cobertura del proveedor de servicio de internet, el servicio no funcionará,
- La documentación almacenada en los equipos de cómputo esta compartida para todos los usuarios sin restricción alguna.
- No existe un Firewall o equipo que haga sus veces.
- Los equipos de cómputo no tienen instalado antivirus, firewall, antimalware, entre otros.
- Los equipos de cómputo no tienen ningún tipo de configuración que pueda brindar seguridad a la máquina y a la red.
- Los usuarios registrados en cada máquina son categoría administrador y no tienen contraseña, por lo cual cualquiera puede ingresar a las máquinas de la red.

8.3.2 Recomendaciones de acciones o controles que se deben realizar para reducir ataques por vulnerabilidades. Una vez elaborado este informe con un inventario de novedades bastante extenso, se puede visualizar la necesidad urgente de comprender el riesgo tan alto al que está expuesta la red de datos, los equipos de cómputo y por ende la información almacenada en los mismos. Estos riesgos y/o vulnerabilidades, se pueden materializar en amenazas y con un nivel de seguridad totalmente nulo ésta red puede ser víctima de atacantes inescrupulosos, quienes con el menor esfuerzo pueden causar un daño de grandes magnitudes con un impacto a nivel nacional e incluso a nivel internacional, ya que la obtención de información sensible como son los últimos descubrimientos de naufragios, los cuales también son buscados por asociaciones internacionales, además de diferentes países que tienen diferentes intereses, pueden afectar las relaciones armoniosas con otras naciones.

Por lo anterior se recomienda realizar los siguientes cambios urgentes, que implican incluso inversión:

8.3.2.1 Red estructurada. Se recomienda contemplar la inversión para una nueva red estructurada, donde se tenga en cuenta toda la normatividad existente para su instalación, esto implica:

- Análisis de requerimiento de puntos estructurados.
- Cambio del cableado utp actual. La categoría del cableado estructurado recomendado es 6 A F/UTP.
- Cambio del cableado eléctrico.
- Levantamiento de planos de la red estructurada incluyendo la red eléctrica, regulada y no regulada.
- Descripción en los planos de la distribución de cargas de las UPS destinada para los equipos de cómputo de la red, se debe dejar debidamente identificada la red eléctrica regulada marquillada, identificado y registrado en el plano la distribución.
- Se debe establecer los puestos de trabajo que se requieren, estos deben incluir punto de voz, datos, toma doble de para energía regulada, toma doble para energía normal, en la realización de este trabajo se debe cumplir con las normas técnicas de marcación.
- Todos los puntos de voz y datos deben ser certificados y probados.
- En caso de cambio de canaleta, se recomienda que esta sea plástica ya que la instalación se realizará en un buque el cual está expuesto a la corrosión por salinidad. En caso de instalar canaleta metálica se recomienda que esta implemente pintura electroestática, división para cableado de red y cableado eléctrico.
- Se recomienda se exija el uso de elementos mono marca (cableado eléctrico, cableado de red, patch cord, faceplate, switch, etc).
- Solicitar garantía del trabajo realizado, mínimo 1 año, garantía del cableado utp mínimo de 10 años, garantía del cableado eléctrico mínimo 1 año.
- Se debe solicitar experiencia que garantice la idoneidad del personal y/o empresa que realizará los trabajos de restructuración dela red.
- Se debe exigir el cumplimiento de las normas en su última actualización para los trabajos de instalación de la nueva red de datos:
    - ANSI/TIA-568-C.0 Generic Telecommunications Cabling for Customer Premises 2009. Norma que dicta las directrices para cableado genérico de telecomunicaciones en instalaciones de clientes.
    - ANSI/TIA-568-C.1 Commercial Building Telecommunications Cabling Standard 2009. Norma internacional que estipula las condiciones del cableado de telecomunicaciones para una edificación comercial
    - ANSI/TIA-568-C.2 Commercial Building Telecommunications Cabling Standard 2009. Norma que crea y estipula directrices de los diferentes

componentes de un sistema de telecomunicaciones basado en transmisión en cables de pares trenzados.
- ANSI/EIA/TIA-606A Guía para marcar y administrar componentes sistema red de datos.
- J-STD-607A Requisitos de unión y puesta a tierra para telecomunicaciones.
- TIA/EIA-854 1000baseTX.
- IEEE 802.3 10baseT Ethernet.
- IEEE 802.3u 100baseTx Fast Ethernet.
- IEEE 802.3ab 1000baseT.
- IEEE 802.3an 10Gbase-T.
- EMI IEC62040-2 / EMS IEC61000-4-2(ESD), IEC61000-4-3(RS), IEC6100-4-4(EFT), IEC6100-4-5.
- ICONTEC NTC 3383 Método de especificación del funcionamiento y requisitos de ensayo de sistemas de potencia ininterrumpida (UPS).
- Reglamento Técnico de Instalaciones Eléctricas (RETIE) que se encuentra en la norma NTC 2050.

- Se debe solicitar patch panel de la misma marca, específico para el cableado utp requerido, mínimo de 24 puertos, cada patch panel debe tener organizador de la misma marca, desde ser debidamente marquillado.
- Se debe exigir que la instalación del cableado utp el manejo de radios de curvatura tipo heavy duty.
- En cuanto a la red eléctrica regulada se debe tener en cuenta lo siguiente:
  - El cableado a utilizar se recomienda de cobre rojo electrolítico 99% de pureza, temple suave y aislamiento termoplástico resistente a la humedad para 600 V tipo THW calibre 12 o 10 según se requiera y 75° C.
  - Los tomacorrientes regulados deben ser dobles monofásicos con polo a tierra aislado de 15 A 125 V, color naranja con terminales de tornillo apropiados para recibir cables hasta No 10 AWG.
  - Los tomacorrientes no regulados serán dobles monofásicos con polo a tierra no aislado de 15 A 125 V, color blanco con terminales de tornillo apropiados para recibir cables hasta No 10 AWG.
  - En el manejo de la conexión de las tomas eléctricas se debe tener en cuenta la posición de la fase, el neutro y la tierra para así tener una correcta polaridad. Lo mismo debe contemplarse en la derivación del circuito para cada tomacorriente, el cual se hará con empalmes cola de rata de tres hilos.
- En cuanto al centro de datos se recomienda el reemplazo del rack de las dimensiones necesarias para los equipos activos de la red. Se debe tener en cuenta que el espacio es muy reducido, el rack que se adquiera se recomienda tenga extractores de calor encerrado, chapa de seguridad.
- Se recomienda el reemplazo de los 02 switch existentes, por unos con soporte de protocolo IPV6, administrable capa 3, mínimo 24 puertos 10/100/1000.

- Se debe realizar revisión y diagnóstico de la ups actual con el fin de determinar si está en condiciones óptimas, si requiere mantenimiento correctivo o si requiere la adquisición de un nuevo equipo.

8.3.2.2. Métodos de protección.

- Requiere de la instalación de un antivirus en cada equipo de cómputo de la red, el cual permanezca actualizado, con reglas como verificación de cada dispositivo que se conecte a la maquina con el fin de buscar posibles malware que puedan contener y restringir su contaminación y propagación por la red.
- Se debe realizar limpieza de cada equipo de cómputo para descartar que tengan rastros de virus.
- Requiere igualmente la instalación en cada equipo de cómputo de una herramienta antimalware que permanezca actualizada y activa.
- Se recomienda la adquisición y correcta configuración de un IPS, a disposición se encuentran IPS de licencia gratuita y de licencia comercial.
- Se recomienda la adquisición y correcta configuración de un FIREWALL, a disposición se encuentran IPS de licencia gratuita y de licencia comercial. Se debe realizar la configuración para asegurar que no se encuentre ningún tipo de vulnerabilidad a través de puertos abiertos.
- Se recomienda migrar el sistema operativo XP a uno más seguro ya que para este sistema el fabricante dejo de emitir actualizaciones de seguridad desde comienzos del año 2014, por lo cual es uno de los sistemas operativos más vulnerables; actualmente Microsoft quien es el fabricante de los sistemas operativos Windows tiene a disposición y de manera gratuita la versión de su sistema operativo Windows 10. Igualmente se recomienda que el sistema operativo que sea instalado se configure para que realice las actualizaciones de seguridad necesarias y sugeridas por el fabricante.
- Para los equipos con sistema operativo Windows 7, como recomendación se debe configurar para que el sistema operativo realice las actualizaciones de seguridad necesarias y sugeridas por el fabricante.
- Se recomienda activar en caso de no adquirir elementos de seguridad informática como firewall e IPS configurar en cada equipo de cómputo el firewall el cual pone a disposición el fabricante del sistema operativo empleado.

8.4 POLÍTICAS DE SEGURIDAD PROPUESTAS.

Se requiere la implementación de políticas de seguridad que permitan proteger y distribuir los recursos de la red de datos del AR LIBERTAD para garantizar la seguridad de las tecnologías de información, como lo son hardware, software, servicios de voz y datos.

Se requiere que las políticas de seguridad definan lo que está permitido y lo que está prohibido, que permita definir los procedimientos y herramientas necesarias, para garantizar el buen uso de los recursos tecnológicos de la red de datos y que sean aplicables para todo el personal que hace uso de la misma y para todos los equipos de cómputo que se conecten a la red. Estas políticas en su gran mayoría están establecidas para las unidades en tierra de la Autoridad Marítima Nacional, para las unidades a flote o buques no se tiene nada implementado.

Se recomienda que las políticas de seguridad comprendan como mínimo los siguientes aspectos:

A. POLITICAS DE SEGURIDAD LOGICA.

I. CONTROLES DE ACCESO A EQUIPOS DE CÓMPUTO, SISTEMAS DE INFORMACIÓN, BASES DE DATOS Y A LA RED.

1. Será responsabilidad de la dirección del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**, establecer una adecuada segregación de funciones dentro de su estructura organizacional en el departamento de informática, estas funciones deben ser asignadas de manera adecuada al personal calificado.
2. Es responsabilidad del departamento de informática del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**, asegurar que cada funcionario tenga asignado unos derechos de acceso a los sistemas de información y recursos informáticos, de acuerdo a sus funciones, que permanezcan actualizados con el nivel de autorización asociado a sus funcionarios y le permitan desarrollar adecuadamente su trabajo.
3. Cada funcionario debe contar con una identificación única e intransferible dentro del sistema de control de accesos. La combinación de usuario y "contraseña" debe ser única.
4. Cada funcionario se hará responsable de las actividades y transacciones que se realicen con su "usuario y contraseña" ya que estos son de carácter confidencial e intransferible. Deben tener claro los aspectos legales que puede acarrear acciones negativas realizadas con su respectivo usuario.

5. Los derechos de acceso de los funcionarios a los sistemas de información y/o bases de datos del BUQUE OCEANOGRÁFICO **“A.R. LIBERTAD”** , deben estar acorde a sus funciones, deben ser autorizadas por la dirección del BUQUE OCEANOGRÁFICO, y será evaluada y avalada por el responsable de la seguridad informática del BUQUE OCEANOGRÁFICO.

6. Los derechos de acceso deben ser asignados de tal forma que no interfieran con las actividades o datos privados de otros funcionarios.

7. Para la “contraseña” asignada al nombre de usuario, se deben tomar las siguientes recomendaciones:

- Las “contraseñas” de usuario deben ser alfanumérica, contener caracteres especiales y una longitud no menor a 8 caracteres, no utilizar espacios en blanco, no deben tener relación con el propietario, como fecha de cumpleaños, nombres de familiares y apellidos, números de identificación, entre otros.
- La contraseña no debe revelarse bajo ninguna circunstancia, ni deben ser reutilizadas.
- El nombre de usuario y la contraseña no puede ser iguales.
- Se debe prohibir el uso de contraseñas cíclicas como por ejemplo meses más el año (abril2016).

8. Está totalmente prohibido que un funcionario autorice el uso de usuario y contraseña a otras personas.

9. Los funcionarios no podrán dejar nombres de usuario y contraseñas escritos en lugares donde puedan ser vistos o tomados por terceros.

10. Cuando se asigne un usuario por primera vez a un funcionario, se debe dar a conocer inmediatamente la política de seguridad del BUQUE OCEANOGRÁFICO.

11. Cuando se asigne un usuario y contraseña por primera vez a un funcionario, el departamento de informática en el directorio activo debe establecer la regla para que el propio funcionario realice el cambio de la misma de forma inmediata.

12. Cada sistema debe contener la información necesaria para identificar cada nombre de usuario con el funcionario responsable de su uso.

13. El departamento de informática deberá establecer regla en el directorio activo para que obligatoriamente cada funcionario realice cambio de contraseña por lo menos cada 45 días.

14. El departamento de informática debe mantener activo el detector de intrusos a cada equipo de cómputo, este deberá restringir el acceso a la

maquina luego de tres (3) intentos de ingresos fallidos. El usuario debe notificar al departamento de informática para su reactivación.

15. El departamento de Informática deberá revisar como mínimo semestralmente los derechos de accesos asignados a los usuarios administradores de los sistemas bajo su responsabilidad grupos de privilegios (incluye personal de la propia oficina, personal técnico, auditor y cualquier otro que lo requiera), se debe verificar estos derechos están ajustados a las funciones y tareas de cada funcionario.

16. Todas las revisiones o modificaciones que se realicen sobre el directorio activo y sobre el controlador de dominio debe quedar debidamente registrado en una bitácora de acciones.

17. Cada vez que un funcionario se ausente de la oficina por vacaciones, incapacidades, licencias y que este tiempo sobrepasen 5 días hábiles el departamento de informática previa información del departamento de talento humano deshabilitara los derechos de acceso del usuario, hasta tanto no se realice el reintegro a sus labores por parte del funcionario.

18. Los funcionarios no deben dejar desatendido el equipo de cómputo, de requerir alejarse del puesto de trabajo, el funcionario debe cerrar los aplicativos o bases de datos sobre las cuales este trabajando, y debe dejar bloqueada la sesión de trabajo.

19. Al terminar la relación laboral de cualquier funcionario (despido, renuncia, incapacidad, traslado a una unidad, etc.), será responsabilidad del departamento de Logístico, informar inmediatamente al departamento de informática para que revoque y deshabilite el usuario y los privilegios otorgados.

20. Se debe mantener en un sobre sellado y bajo la responsabilidad del Responsable del departamento de informática, un código de usuario de contingencia y su respectiva contraseña que posea todos los privilegios del Administrador de la Red, Administrador de Base Datos u otros, para ser utilizado solamente en caso de emergencia. En caso de requerir su uso debe quedar debidamente registrado. Esta contraseña debe ser actualizada mínimo cada seis meses.

21. El departamento de informática debe prohibir lógicamente las sesiones múltiples de un usuario de red, este debe ser un privilegio exclusivo de administradores del sistema.

II. USO DE LOS EQUIPOS Y SERVICIOS.

1. Los funcionarios tienen prohibido almacenar juegos y utilizar los equipos de cómputo del BUQUE OCEANOGRÁFICO para este tipo de actividades.

2. Los equipos de cómputo, aplicaciones, bases de datos y toda la información del BUQUE OCEANOGRÁFICO no podrán utilizarse para fines personales.

3. Todos los funcionarios tienen prohibido suministrar los equipos de cómputo, aplicaciones, bases de datos y toda la información del BUQUE OCEANOGRÁFICO a personas externas o sin vínculo laboral con el BUQUE OCEANOGRÁFICO.

4. Se prohíbe a todos los funcionarios el uso de aplicativos y bases de datos, información para dañar, deteriorar o alterar los activos del BUQUE OCEANOGRÁFICO.

III. CONTROL DE SOFTWARE MALIGNO.

1. Con el fin de evitar daños al parque computacional, equipos activos de la red, información, aplicativos, bases de datos entre otros, el departamento de informática deberá gestionar ante la dirección, la compra de software debidamente licenciado como son, antivirus, antimalware, antispyware.

2. La dirección del BUQUE OCEANOGRÁFICO, está debe atender las sugerencias del departamento de informática para obtener el mejor software para proteger su parque computacional, equipos activos de la red, información, aplicativos, bases de datos entre otros.

3. El departamento de informática deberá configurar en todos los equipos de cómputo el software adquirido para control de software maligno , de forma tal que funcione su actualización y verificación de dispositivos automáticamente, se recomienda contar con un servidor desde donde se puedan establecer y configurar todas las políticas necesarias para evitar algún tipo de daño por software maligno.

4. Los funcionarios deberán informar inmediatamente al departamento de informática, sobre cualquier novedad que observen sobre el funcionamiento o detecciones de este tipo de software de protección, no deben tomar acciones propias.

5. Se prohíbe a los funcionarios la instalación de software libre o licenciado obtenido por cualquier medio, solo se podrá contar con el software establecido por la dirección del BUQUE OCEANOGRÁFICO y el departamento de informática.

6. El departamento de informática deberá configurar sobre el servidor de antivirus la restricción de uso de puertos usb, y el acceso a dispositivos usb, en todo el parque computacional, solo tendrán permisos aquellos

funcionarios a quienes se les realice estudio y por la naturaleza de sus funciones lo requieran y sea de vital importancia.

7. Todos los funcionarios deben descomprimir información recibida y hacer revisión para corroborar que no son archivos contaminados, antes de abrirlos y utilizarlos.

8. El departamento de informática debe configurar un sistema de protección contra escritura en cada equipo de cómputo y servidores con el fin de proteger sus activos en caso de que una maquina sea contaminada por un software maligno.

9. En cada mantenimiento preventivo y/o correctivo que se realice al parque computacional por el funcionario o empresa encargada de esta función, se debe verificar la instalación del software de control de software maligno, su actualización y correcto funcionamiento.

IV. PROCESO DE CONTROL DE CAMBIOS.

1. En cada mantenimiento preventivo y/o correctivo que se realice al parque computacional por el funcionario o empresa encargada de esta función, se debe verificar estado y actualización de los sistemas operativos, igualmente se debe verificar que solo este instalado el software autorizado por el departamento de informática del BUQUE OCEANOGRÁFICO. En caso de encontrar software no autorizado debe registrarlo en la bitácora de mantenimiento e informar inmediatamente al departamento de informática para que tomen las acciones procedimentales y legales correspondientes.

V. OPERACIÓN DEL COMPUTADOR.

1. Se prohíbe fumar, comer y beber en el centro de cómputo e instalaciones con equipos tecnológicos.

2. Se prohíbe a todos los funcionarios fumar, beber, comer cerca de cualquier equipo que haga parte del parque computacional, sea o no el asignado.

B. POLÍTICA DE RESPALDOS Y RECUPERACIÓN.

1. El departamento de informática deberá definir el personal autorizado y responsable para la realización de los diferentes respaldos que la información del BUQUE OCEANOGRÁFICO y sus funcionarios requieran. Este personal también debe estar en la capacidad de recuperar la información cuando sea necesario.

2. En el respaldo de los datos se debe considerar tanto los datos de la aplicación (archivos, bases de datos, datos estructurados y no estructurados) como los demás elementos necesarios para asegurar la prestación de servicios, tales como el software de la aplicación (programas) y parámetros de operación, documentación complementaria a los procesos, sistemas operativos, software de ambiente y demás.

3. El departamento de informática debe crear un cronograma de la programación del proceso de respaldo (diario, semanal, mensual y anual), además se debe contar con procedimientos de verificación y supervisión de los procesos y del contenido de los respaldos.

4. Todos los procesos de respaldo y recuperación de información deben proveer los elementos que evidencien (log de eventos) la ejecución del proceso, detalle del contenido de los mismos, así como deficiencias en caso de existir.

5. Los medios de respaldo deben ser protegidos de borrados accidentales a través del uso de medios físicos y lógicos de carácter preventivo (“lock” en los medios de Backup, otros).

6. Los medios de respaldo se deben etiquetar, las etiquetas deben tener información de su contenido, nombre, fecha del respaldo y funcionario que lo realizó.

7. Los respaldos de datos y demás elementos necesarios, deben estar almacenados en sitios que dispongan de condiciones de acceso restringido y de medio ambiente apropiado a los medios utilizados, así como para hacer frente con éxito a eventos contingentes como incendios, inundaciones u otros.

8. Antes de proceder a la restauración de datos sensibles o críticos a partir de un respaldo se debe realizar una copia de los mismos para minimizar efectos de corrupción o daños de los datos originalmente respaldados.

9. Se debe generar una copia de todos los respaldos, los cuales se custodiarán en un sitio alterno, que cumpla con las características y protección ambiental similares al sitio principal. La proximidad entre el sitio principal y el alterno se debe contemplar dentro de los parámetros que se establezcan en el convenio de salvaguarda y custodia de información. Se recomienda disponer al menos de dos vías de acceso distintas.

10. Se deben tomar las medidas de seguridad necesarias para el traslado de los medios de respaldo al sitio alterno, a fin de garantizar no solo que llegarán a su destino sino la integridad de los medios.

11. Como mínimo semestralmente se debe verificar la validez de los respaldos custodiados en el sitio principal y en sitio alterno. Se debe verificar la

condición de los medios de almacenamiento y si los datos pueden ser restaurados oportuna y confiablemente.

12. A los equipos y los medios usados para el respaldo se les debe realizar periódicamente mantenimiento preventivo por parte del personal encargado de esta función. Se debe asegurar correcto funcionamiento de los mismos.

C. SEGURIDAD DE REDES LAN.

1. El responsable del departamento de informática del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**, debe nombrar un responsable para la administración de la red LAN - WIFI, cuyas funciones y tareas deben estar claramente definidas y delimitadas.

2. Todo el parque computacional (computadoras, estaciones de trabajo, estaciones gráficas, servidores y equipo accesorio, dispositivos móviles, tabletas, Smartphone), que esté o sea conectado a la Red del BUQUE OCEANOGRÁFICO, o aquel que en forma autónoma se tenga y que sea propiedad del BUQUE OCEANOGRÁFICO, o que use la red de datos del BUQUE OCEANOGRÁFICO debe sujetarse a las normas y parámetros de instalación y configuración que emita el departamento de informática del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**.

3. El departamento de informática debe contar con un inventario actualizado de los activos informáticos propiedad del BUQUE OCEANOGRÁFICO y también inventario de los equipos que no pertenezcan a EL BUQUE OCEANOGRÁFICO pero estén conectados a la red, con la información del funcionario responsable, software instalado, permisos de usuario y todo lo que corresponda a cada elemento.

4. El departamento de informática coordinará con el funcionario encargado del mantenimiento preventivo y correctivo del parque computacional, la realización de estas tareas, así como la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir los procesos internos respectivos y relacionar dichas tareas en el sistema de información destinado para ello.

5. El departamento de informática debe proteger con medios físicos (tales como candado, etiquetas u otros) aquellos equipos o sus componentes que por su valor o exposición pueden estar sujetos a pérdidas o sustracción.

6. La adquisición de hardware y software sebe ser gestionada a través del departamento de informática en conjunto con el departamento administrativo bajo las directrices y normativas técnicas.

7. Todo el parque computacional debe ser objeto de mantenimiento preventivo y/o correctivo, se debe programar anualmente un cronograma por el departamento de informática.

8. En los equipos de cómputo del BUQUE OCEANOGRÁFICO, únicamente se debe instalar el software debidamente autorizado por el departamento de informática y para el que se disponga de las licencias de uso respectivo.

9. Está prohibido el uso del software y recursos informáticos propiedad del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**, para fines ajenos a las actividades propias del BUQUE OCEANOGRÁFICO.

10. El funcionario del encargado del mantenimiento preventivo y correctivo del parque computacional serán responsable del soporte y buen funcionamiento de los equipos de cómputo de la red del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**, bajo la supervisión del responsable departamento de informática, según los términos establecidos en la contratación del servicio y deben asegurar que las condiciones de medio ambiente en que operan éstos se ajustan a las establecidas por departamento de informática.

11. Se debe contar con documentación actualizada sobre los componentes y organización de la red de datos del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"** y de los recursos asociados a ésta, entre otros: enlaces y diapositivas de conexión físicas, protocolos de comunicaciones y direcciones IP, segmentaciones de la LAN extendida y canales de comunicación.

12. Los requerimientos para la instalación y actualización de redes deben ser formalizados y controlados adecuadamente, asegurando que su ejecución no interfiera con la operación normal de los servicios.

13. El departamento de informática debe contar con Sistema de detección de intrusos instalados y correctamente configurados para evitar vulnerabilidad en la red y en sus equipos.

14. El departamento de informática debe contar con Sistema de Prevención de intrusos instalados y correctamente configurados para evitar vulnerabilidad en la red y en sus equipos.

15. El departamento de informática debe contar con Firewall instalados y correctamente configurados para evitar vulnerabilidades de la red.

D. POLÍTICAS DE ACCESO Y USO DE WIFI.

La administración de los recursos de tecnologías de la información y las comunicaciones es importante para el cumplimiento y desarrollo de labores en el BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**.

Las redes inalámbricas requieren de un alto grado de responsabilidad por parte de los usuarios de la red para aprovechar y maximizar los beneficios de la tecnología, brindando cobertura de red inalámbrica y un sistema de comunicaciones seguro para el buque Oceanográfico.

El departamento de informática deberá difundir las políticas entre los usuarios de los recursos. A continuación se definen las políticas relacionadas con la red inalámbrica WLAN:

1. El departamento de informática establecerá los procedimientos para la instalación, administración y configuración de la red inalámbrica de la entidad, con el fin de mantener la integridad, seguridad de la información así como la seguridad de la infraestructura de red LAN y WLAN.
2. Los equipos y antenas inalámbricas única y exclusivamente deberán ser instalados por personal del departamento de informática o por personal avalado por el departamento de informática, así como su supervisión y monitorización de uso.
3. El departamento de informática debe evitar el mal uso de la red inalámbrica del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**, así como el acceso a sistemas o aplicaciones no autorizadas (Redes Sociales, reproducción de videos, juegos en línea, descarga de aplicativos) que afectan el desempeño de la red inalámbrica diseñada y destinada con fines netamente laborales.
4. El departamento de informática monitoreara las páginas visitadas, y las mismas serán restringidas a través de los perfiles de navegación definidos en esta política.
5. El departamento de informática debe regular y controlar la instalación de equipos inalámbricos externos a la red del BUQUE OCEANOGRÁFICO como equipos móviles de comunicación para prevenir la interferencia con otros usuarios que utilicen el mismo espectro de frecuencias.
6. El departamento de informática restringirá la propagación de SSID de dispositivos de anclaje, como modem 3G, 4G, y zonas de anclaje de celulares Smartphone.
7. El departamento de informática debe monitorear y generar reportes de tráfico de los usuarios de la red Inalámbrica del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**.

E. POLÍTICAS DE ACCESO Y USO DE INTERNET.

1. Es responsabilidad de cada usuario el uso prudente de las tecnologías como el internet, que el BUQUE OCEANOGRÁFICO coloca a su disposición.
2. Se prohíbe a todos los funcionarios el acceso a sitios de Internet que no tengan relación alguna con los objetivos del BUQUE OCEANOGRÁFICO, como son: pornografía, racismo, apuestas, actividades criminales, drogas, juegos, y cualquier otra que se estime conveniente restringir, en relación al uso de buenas prácticas y sanitización de la red.
3. No se autoriza a los funcionarios acceder a sitios para el establecimiento de charlas, salvo que tengan relación alguna con las funciones que desempeña, para ello el departamento de informática hará las respectivas configuraciones.
4. Sólo funcionarios con previa autorización podrán "descargar" información desde Internet, esto se hará bajo la supervisión y monitoreo del departamento de informática.
5. Toda información descargada de Internet debe estar relacionada con los objetivos del BUQUE OCEANOGRÁFICO y las funciones que lleva a cabo el usuario.
6. Todos los archivos obtenidos desde Internet deben ser revisados para detección de virus previo a ser descargados en cualquier computador.
7. Ningún documento, información, software, no puede ser transferida a terceros sin autorización y un compromiso de confidencialidad entre el BUQUE OCEANOGRÁFICO y terceros.
8. El tiempo de acceso a Internet no debe interferir ni distraer a los usuarios de sus funciones normales.
9. Toda información que transite por la red del BUQUE OCEANOGRÁFICO se considera propiedad exclusiva del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**.
10. La información transmitida, procesada producto de las funciones del personal y que concierne al BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"**, o a sus funcionarios, no podrá ser interceptada o divulgada bajo ninguna circunstancia, por ningún usuario interno de la red del BUQUE OCEANOGRÁFICO, salvo en aquellos casos que los organismos de seguridad establezcan bajo órdenes judiciales.

F. SANCIONES.

Cualquier violación a la política de Seguridad informática del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"** deberá ser sancionada de acuerdo al Reglamento Interno de Trabajo, igualmente se tendrán en cuenta las normas, leyes y estatutos de la ley Colombiana como lo es *La Ley 1273 de 2009, entre otras.*

El departamento de informática debe elaborar un informe preliminar a la Dirección del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"** , con copia a quien corresponda con las infracciones a la seguridad correspondiente, con el fin de que se tomen las acciones normativas que correspondan a quienes violen las disposiciones en materia de informática del BUQUE OCEANOGRÁFICO.

Todas las acciones en las que se comprometa la seguridad de la Red del BUQUE OCEANOGRÁFICO **"A.R. LIBERTAD"** y que no estén previstas en esta política, deberán ser revisadas por el departamento de informática, para dictar una directiva sujetándose al estado de derecho.

9. RESULTADOS E IMPACTOS

9.1 RESULTADOS

Con el desarrollo de este proyecto se logra obtener los siguientes resultados:

Con la aplicación de herramientas de pentesting como Nmap, GFI LandGuard 2015, se pudo evidenciar el grado de vulnerabilidad tan alto que tiene la red de datos y los ordenadores que la componen, se pudo evidenciar la carencia de software que impida la contaminación de las maquinas con virus, troyanos, que puedan llegar a generar intrusiones y vulnerabilidad a unos de los pilares de la informática como lo es la confidencialidad.

Estas herramientas permitieron realizar un análisis que determinó que el 100% de los equipos de cómputo de la red tienen un nivel de riesgo de 10 sobre 10 de ser víctima de ataques informáticos los cuales se pueden llevar a cabo de diferentes maneras y sin mucho esfuerzo ya que no cuentan con ningún sistema de seguridad.

Las herramientas utilizadas para el análisis de vulnerabilidad fueron de gran ayuda para la obtención de datos gracias a su practicidad.

Se presenta un informe con una serie de recomendaciones las cuales requieren de una gran inversión, sin embargo esta inversión redundara en la protección de uno de los recursos más importante para esta embarcación y para la nación como lo es la información y el hardware.

Se puede observar la necesidad urgente que tiene la red de datos y el parque computacional del buque A.R. LIBERTAD, de contar con un sistema de Prevención de Intrusos y de un Firewall o configuración del firewall en cada máquina que haga parte de la red de datos, sin estas herramientas aunque se instale un software que prevenga software maligno, tendrán presente el riesgo de un ataque informático de forma directa.

Se logra presentar unas políticas de seguridad informática con las cuales no contaba el buque A.R. LIBERTAD aunque en gran parte están establecidas por la Autoridad Marítima nacional y las cuales servirán para fortalecer la seguridad de los equipos de cómputo y de la red de datos, con estas políticas se tendrá una mejor administración de los recursos y disminuirá en un gran porcentaje el nivel de vulnerabilidad de la red. Sin embargo se requiere un compromiso por parte del comandante del buque, y del funcionario encargado de ejercer las funciones de sistemas informáticos para hacer cumplir estas políticas y lograr con eficiencia mitigar la mayoría de los riesgos a los que se ven expuestos actualmente.

Este proyecto en su totalidad está dirigido al fortalecimiento de la seguridad informática en una red de datos que se encuentre implementada en cualquier tipo de infraestructura. Por tanto puede ser usado para implementarse en los demás buques oceanográficos con los que cuenta la Autoridad Marítima de Colombia.

9.2 IMPACTOS

Uno de los impactos que ha generado la realización de este proyecto es la concienciación tanto del comandante, como de toda la tripulación del buque A.R LIBERTAD, incluso mandos superiores; Al comprender el nivel de riesgo en el que sé que encuentra la red de datos y el nivel de exposición para que un ataque informático se realice, aceptan las recomendaciones dadas e incluso se pudo servir de puente para corregir las fallas que inmediatamente se pueden solucionar así:

- Se realiza con apoyo de un personal de soporte técnico mantenimiento preventivo y correctivo; se ejecutan herramientas para la verificación y eliminación de software maligno, en todas las máquinas, se eliminan virus y troyanos identificados en varias máquinas.

- Igualmente se realiza actualización de cada sistema operativo de los ordenadores de la red.

- Se realiza activación del firewall de cada ordenador conectado a la red de datos.

- Se solicitó al Departamento de Informática de la Autoridad Marítima, sede central el software legal que se utiliza para prevenir software maligno se obtuvo respuesta y envían:
  - Antivirus Licenciado.
  - Anti espía Licenciado.
  - Agente de red licenciado.

  Este software fue instalado en cada una de las máquinas y configurado de tal manera que se actualice automáticamente y verifique los dispositivos que se conecten al ordenador con el fin de buscar software maligno y eliminarlo.

- Se realiza levantamiento de hoja de vida por elemento del parque computacional y elementos activos de la red con el fin se realice registro de novedades sobre cada una de estas y se pueda llevar un mejor control de cada elemento.

Otro impacto importante que se obtuvo con la realización de este proyecto es el apoyo de la dirección general para fortalecer el tema de seguridad informática es por ello que actualmente se están adelantando las siguientes tareas:

- Se está apoyando a la unidad, con la investigación de empresas que puedan realizar los trabajos de readecuación y dotación de elementos activos de la red, esto con el fin de obtener cotizaciones de costos y poder solicitarlos en anteproyecto.
- Se está apoyando con un proyecto de renovación del parque computacional, el cual contara con sistemas operativos actualizados y legales, se configurará el firewall de la máquina para que soporte el tema de seguridad y se les instalará el software para prevenir software maligno

Y se está trabajando en uno de los planes más ambiciosos, por la tecnología e inversión que implica, se está apoyando con un proyecto de conectividad de la red del Buque oceanográfico con la red de la sede central de la Autoridad Marítima, este proyecto busca reemplazar el modo de conexión a internet y brindar una conexión inalámbrica que permita obtener servicios de voz y datos de acuerdo a los parámetros establecidos para cada una de las oficina ubicada en tierra y con posibilidad de conexión desde cualquier lugar del mundo, ya que estos buques serán empleados para las nuevas investigaciones que realizará el país en la Antártida, esto permitirá que la sede central y los centros de investigación que requieren la información la obtengan en tiempo real, pueda ser monitoreada y además con el servicio de privacidad, confidencialidad, integridad que actualmente tienen otros elementos del estado como lo es el servicio de conectividad del avión presidencial de Colombia.

Se proyecta contar con un servicio de red inalámbrica que cuente con un controlador que permita identificar interferencia y ordene a los Access Point que se pongan a disposición de la red para que cambien de canal y así evitar interferencias, también se busca que se puedan detectar y evitar intrusos que pretendan acceder a la red y a la información, al igual que ataques que pretendan tumbar la red, además de los temas de seguridad informática que tiene establecidas las oficinas en tierra de la Autoridad Marítima.

Estos proyectos cuentan con el aval del comandante del buque A.R. LIBERTAD y se presentarán para el anteproyecto 2016 con adquisición de vigencia 2017, se prevé que se solucionen los temas de seguridad y se desarrollen los proyectos propuestos a corto plazo.

Este proyecto generó gran interés al punto de que va a implementarse en los demás buques oceanográficos que conforman la flota de investigación marina de Colombia.

9.3 AVANCE DE RESULTADOS.

En la siguiente tabla se hace un resumen de las vulnerabilidades encontradas en la red de datos del buque oceanográfico A.R LIBERTAD, se especifica aquellas que ya fueron solucionadas y la medida adoptada, igualmente se relacionan las novedades que fueron aceptadas y sobre las cuales no se puede tomar una acción inmediata ya que se requiere asignación de recursos económicos para la solución, estos últimos fueron enviados a la sede central de la Autoridad Marítima y serán atendidas en el transcurso del año 2017 y 2018 de acuerdo al presupuesto que asigne la Nación.

Tabla 6. Resumen de vulnerabilidades encontradas.

ESTADO DE LA RED				
Item	**Estado de la red**	**Identificación las vulnerabilidades**	**Vulnerabilidades solucionadas**	**Novedades aceptadas y pendiente para cambios**
1	Estado físico de la red	Cableado estructurado en mal estado	-	Implementación nueva red
2		Cableado estructurado sin marcar	-	Implementación nueva red
3		Planos de la red inexistentes	-	Implementación nueva red
4		Energía regulada con sobre voltaje	-	Implementación nueva red
5		Gabinete de comunicaciones en mal estado	-	Implementación nueva red
6		Equipos activos mal estado	-	Implementación nueva red
7		Patch panel sin marcar	-	Implementación nueva red
8		Cableado utp sin etiquetar	-	Implementación nueva red
9		Seguridad física perimetral deficiente	-	Implementación nueva red
10	Controles y/o medidas establecidas para la seguridad de la red	Políticas de seguridad informática no establecidas	Se presentan políticas de seguridad ajustadas a una unidad a flote y son aceptadas e implementadas	
11		No existen restricciones de navegación hacía internet		
12		Documentación almacenada compartida sin restricción		-

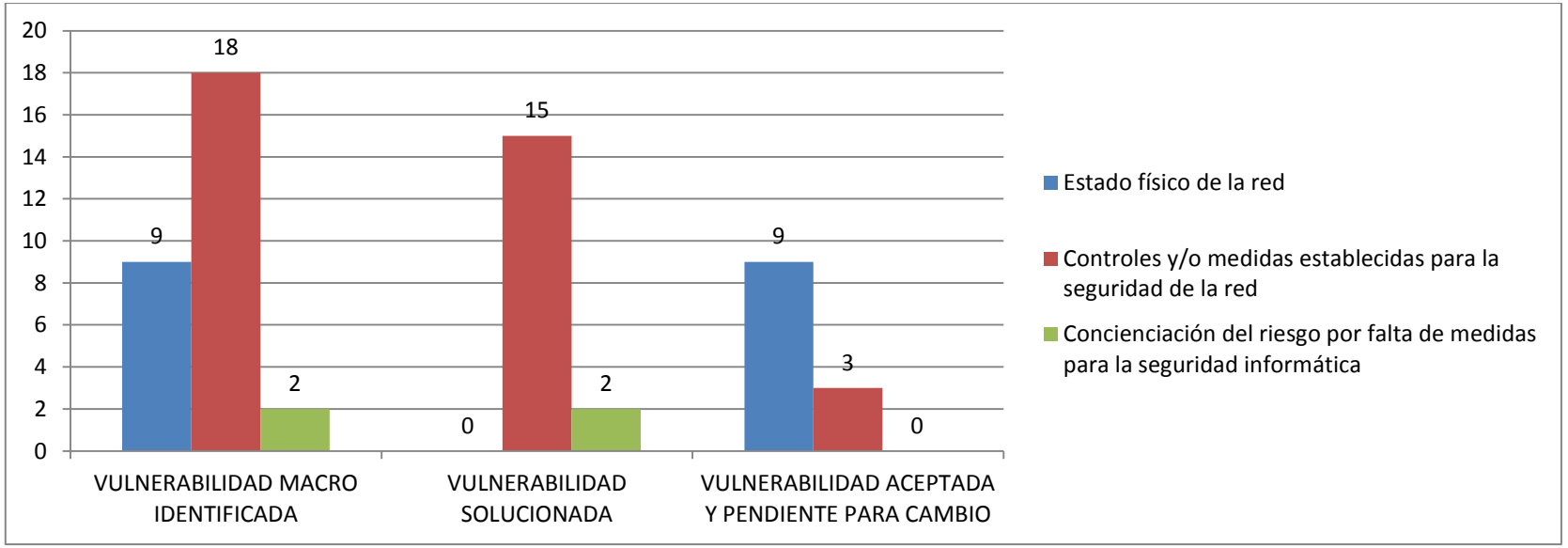
13		No existe un firewall o equipo que haga sus veces.	Se configura firewall en cada maquina	.
14		No existe un sistema de identificación de intrusos, ni físico, ni lógico.		Adquisición de tecnología para este fin
15		No existe un sistema de prevención de intrusos, ni físico, ni lógico.		Adquisición de tecnología para este fin
16		La red de datos no cuenta con un firewall, ni tipo hardware ni tipo software.		Adquisición de tecnología para este fin
17	Controles y/o medidas establecidas para la seguridad de la red	Los equipos de cómputo no tienen instalado antivirus	Se instala y configura software establecido por la entidad	-
18		Los equipos de cómputo no tienen configurado un firewall	Se configura firewall en cada maquina	-
19		Los equipos de cómputo no tienen instalado antimalware	Se instala y configura software establecido por la entidad	-
20		Los equipos de cómputo no tienen instalado agente de red.	Se instala y configura software establecido por la entidad	-
21		Usuario registrado en cada máquina solo administrador sin contraseña.	Se asigna un usuario estándar a cada funcionario. Usuario administrador solo para informática	-
22		71% sistemas operativos obsoletos	Se actualizan los equipos de cómputo a win 10	-
23		Ninguna restricción establecida para uso de la red	Se presentan políticas de seguridad ajustadas a la nave	-
24		Existencia de un troyano.	Se eliminan los troyanos detectados en las maquina	-
25		Puertos abiertos	-	Adquisición de tecnología para este fin
26		Existencia de virus	Se eliminan los virus detectados en las maquina	-
27		Sistemas operativos sin actualizaciones de seguridad	Se configura actualización automática	-

28	Concienciación del riesgo por falta de medidas para la seguridad informática	Falta de conciencia del riesgo que se presenta en la red de datos del buque A.R LIBERTAD	Se logra la comprensión del riesgo al que está expuesta la red de datos y la información del buque A.R LIBERTAD por parte de los directivos	-
29			Se logra la comprensión del riesgo al que está expuesta la red de datos y la información del buque A.R LIBERTAD por parte de la tripulación.	-

Fuente: El Autor

A través de la siguiente figura se puede concluir que el trabajo desarrollado ha permitido contribuir de manera inmediata a la solución de una gran parte de las vulnerabilidades identificadas.

Figura 28. Resumen de vulnerabilidades encontradas.



Fuente: El Autor

En su gran mayoría las vulnerabilidades identificadas en la red LAN del buque oceanográfico A.R LIBERTAD están dentro del marco Controles y/o medidas establecidas para la seguridad de la red, se hallaron 18 vulnerabilidades de las cuales se lograron corregir 15, lo que obedece a un 83.3% de las encontradas en dicho marco; a nivel general se puede afirmar que con la realización de este trabajo se logró corregir el 51.72% del total de las vulnerabilidades identificadas; las restantes solo son subsanables con inyección de un rubro presupuestal el cual está bajo la responsabilidad de la Autoridad Marítima.

Igualmente permite concluir que las vulnerabilidades identificadas son aceptadas y en su totalidad la Autoridad Marítima Nacional serán atendidas teniendo en cuenta las recomendaciones.

10. DIVULGACION

Con el fin de dar a conocer el presente proyecto se realizará un documento que será enviado a las directrices de la organización. Se selecciona este canal de comunicación teniendo en cuenta que el proyecto involucra información confidencial.

11. CRONOGRAMA

ACTIVIDADES PLANTEADAS	SEMANA												
	1	2	3	4	5	6	7	8	9	10	11	12	13
Inicio de Proyecto aplicado													
Revisión observaciones planteadas por tutor													
Planeamiento trabajo en sitio													
Recolección de información													
Aplicación Pentesting a la red LAN													
Sistematización de resultados													
Análisis de resultados													
Redacción del Documento													
Presentación Documento al tutor para revisión													
Entrega del documento en versión digital e impresa para evaluación del jurado													
Corrección del documento													
Entrega del documento final al tutor del curso													

BIBLIOGRAFÍA

Universidad Autonoma de Occidente, Estructura organizacional de la Universidad Autónoma de Occidente [en línea]. Santiago de Cali: Universidad Autónoma de Occidente, 2005. Disponible en Internet: http://bach.uao.edu.co:7778/portal/page?_pageid=83,42714&_dad=portal&_PORTAL

GOBIERNO DE ESPAÑA – MINISTERIO DE DEFENSA Revista General de Marina [en línea]. [s.l]: MINISTERIO DE DEFENSA DE ESPAÑA, 2015. P. 111 – 112. Disponible en Internet: http://publicaciones.defensa.gob.es/pprevistas/dfa2a36b-fb63-65ab-9bdd-ff0000451707/index.html#/112/

ESAU. A, Que es el Pentesting. [en línea]. Sevilla: OpenWebinars, 2015. Disponible en Internet: https://openwebinars.net/que-es-el-pentesting/

INFORMATICAHOY, Que es Hardware y Software. [en línea]. [s.l]: INFORMATICAHOY, 2012. Disponible en Internet: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-Hardware-y-Software.php

NMAP, NMAP [en línea]. [s.l]: NMAP.ORG, [s.f]. Disponible en Internet: https://nmap.org/

TENABLE NETWORK SECURITY, Nessus [en línea]. [s.l]: Tenable Network Security, 2016. Disponible en Internet: www.nessus.org

RAPID 7, Metasploit [en línea]. [s.l]: RAPID 7, 2016. Disponible en Internet: http://www.metasploit.com/

UNIVERSIDAD AUTONOMA DE OCCIDENTE, Instructivo presentación trabajos de grado [en línea]. Cali: UNIVERSIDAD AUTONOMA DE OCCIDENTE, 2015. Disponible en Internet:

http://www.uao.edu.co/sites/default/files/Biblioteca/ArchivosPDF/DocumentosPDF/INSTRUCTIVO_PRESENTACION_TRABAJOS_DE_GRADO.pdf

Unipamplona, NORMA TÉCNICA COLOMBIANA - NTC 1486. [en línea]. [s.l]: Universidad de Pamplona, [s.f]. Disponible en Internet: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

CONGRESO DE LA REPUBLICA DE COLOMBIA, Ley 1273 de 2009 [en línea]. Bogotá: CONGRESO DE LA REPUBLICA DE COLOMBIA, 2009. Disponible en http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL – REPUBLICA DE COLOMBIA, Documento CONPES 3701 [en línea]. Bogotá: CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL – REPUBLICA DE COLOMBIA, 2011. Disponible en http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

ICONTEC, Documento Norma Técnica Colombiana NTC 5254 [en línea]. [s.l]: CORPONOR, 2006. Disponible en: http://www.corponor.gov.co/NORMATIVIDAD/NORMA%20TECNICA/Norma%20T%E9cnica%20NTC%205254.pdf

Auditoria y Seguridad Informática, GFI LanGuard [en línea]. [s.l]: Auditoría y Seguridad Informática SA CV, 2001. Disponible en http://www.auditoria.com.mx/GFI-LanGuard

PAESSLER, “PRTG: Instalado en segundos. Configurado en minutos. Protege redes por años." [en línea]. Nuremberg: Paessler AG, 1998 - 2016. Disponible en https://www.es.paessler.com/prtg

WAXOO, Look@LAN Network Monitor [en línea]. [s.l]. WAXOO S.L, 2013. Disponible en http://looklan-network-monitor.waxoo.com/

ICONTEC, NORMA TÉCNICA COLOMBIANA NTC 5613 [en línea]. Bogota: Instituto Colombiano de Normas Técnicas y Certificaciones (ICONTEC), 2008. Disponible en: http://ieluispatronrosano.santiagodetolu-sucre.gov.co/apc-aa-files/34633230373666653234326333616264/Norma_ICONTEC.pdf

UNILIBRECUCUTA, CITAS Y BIBLIOGRAFÍA - GUIA SOBRE LA FORMA COMO SE ELABORAN CITAS BIBLIOGRAFICAS Y NOTAS DE PIE DE PAGINA [en línea]. Cucuta: UNILIBRECUCUTA. Disponible en: http://www.unilibrecucuta.edu.co/portal/images/investigacion/pdf/Guia_para_Citas_Bibliograficas.pdf

Cienciatec.org, Difusión y divulgación científica en Internet [en línea]. Asturias: Cienciatec.org, 2011. Disponible en: http://www.cienciatec.org/difusion-y-divulgacion-cientifica-en-internet/