Resumen Analítico del Informe Final de Investigación, RAE

Tema	SEGURIDAD INFORMATICA
Título	IDENTIFICACION DE VULNERABILIDADES DE LA RED LAN DEL BUQUE OCEANOGRÁFICO DE LA AUTORIDAD COLOMBIANA A TRAVÉS DE LAS HERRAMIENTAS DE PRUEBAS DE PENTESTING.
Nombres y Apellidos del Autor	Aydee Mercedes Viver Ramírez
Año de la publicación	2017

Fuente bibliográfica:

En el proceso de investigación se consultaron diferentes fuentes relacionadas con el tema de seguridad informática y el uso de herramientas de pentesting para la identificación de vulnerabilidades, la relación de algunas fuentes consultadas son:

- 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/

- 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

- 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

Resumen:

El presente proyecto aplicado tuvo como objetivo identificar las vulnerabilidades de la red LAN del buque oceanográfico A.R. LIBERTAD, a través de herramientas de pentesting con la finalidad de presentar unas recomendaciones que permitan garantizar la seguridad de la información y del parque computacional de dicha red.

Una vez empleadas algunas herramientas de pentesting, se puede evidenciar que actualmente la red de datos del buque oceanográfico A.R. LIBERTAD tiene demasiadas vulnerabilidades, no cuenta con ningún sistema de protección como pueden ser firewall, IDS, IPS, antivirus, antimalware, antispyware, los equipos de cómputo no tienen habilitado el firewall que ofrece el sistema operativo, se evidencia puertos tcp y udp abiertos los

cuales ponen el riesgo la seguridad de los mismos, algunos equipos ya están infectados con software malicioso como son virus, troyanos y spyware.

En cuanto a la red estructurada y todo lo que la compone se evidencias grandes fallas en cuanto al tendido y organización del cableado utp y el cableado eléctrico, no se aplican correctamente las normas establecidas para este tipo de redes.

Dentro de las recomendaciones dadas en el proyecto las cuales están basadas en las novedades y vulnerabilidades detectadas, está la necesidad de establecer políticas de seguridad que permitan establecer parámetros y límites para los usuarios, el uso de los recursos y establecer procedimientos seguros los cuales en este momento son inexistentes; se recomienda la reinstalación de cableado estructurado aplicando normas actuales y con modernización en sus equipos de comunicación que permitirá un mejor desempeño de la red; adquisición y configuración de elementos de seguridad como son firewall, IPS, antivirus, Antimalware, actualizaciones de los sistemas operativos, este conjunto de recomendaciones van dirigidas a fortalecer la seguridad informática de dicha red.

Palabras Claves	Vulnerabilidades de la red de datos, Pruebas de Pentesting a la red de datos, Nmap, GFI LanGuard 2015 Redes de datos, Seguridad informática

Contenidos

En el presente proyecto aplicado se abordaron aspectos y temas importantes sobre la identificación de vulnerabilidades en una red LAN a través de herramientas de pentesting, igualmente se analizaron acciones correctivas que deberían implementarse con el fin de contar con una red de datos segura.

Descripción del problema de investigación:

El problema que se aborda es la situación actual del buque oceanográfico A.R LIBERTAD una unidad a flote de la Autoridad Marítima Colombiana, en lo que respecta a la red de datos con la que cuenta, el interrogante es si la red de datos es segura teniendo en cuenta la importancia de la labor que desempeña el buque y la gran importancia y trascendencia que tiene la información que obtiene este buque en el ejercicio de las funciones asignadas.

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.

Metodología

El presente proyecto aplicado se basó en una metodología de investigación fundamental, se desarrolló a través de un proceso de recolección de información, planificación de procedimientos, ejecución de tareas, análisis de información obtenida, todo esto para obtener unos resultados que permitan presentar una propuesta de acciones correctivas que vayan encaminadas al fortalecimiento de la seguridad informática tanto de la red LAN como de la información que allí se maneja.

Principales referentes teóricos y conceptuales

Dentro de los principales referentes teóricos y conceptuales contemplados en el presente proyecto aplicado se definen los siguientes:

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.

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.

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.

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).

Resultados y conclusiones

Se realizó la verificación del estado de la red LAN del Buque Oceanográfico A.R. LIBERTAD con la finalidad identificar vulnerabilidades y presentar recomendaciones en cuanto a seguridad informática; para ello se efectuó verificación física de la red, esta verificación arrojo como resultado demasiadas fallas en su parte estructurada, fallas en cuanto a seguridad física y perimetral aun cuando se encuentra en una unidad militar; En cuanto a la verificación lógica, esta se realizó través de herramientas de pentesting. Una vez culminada revisión se pudo 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, que vayan dirigidas a la reglamentación y uso adecuado de la red, no existen restricciones de navegación hacía internet, la documentación almacenada en los equipos de cómputo está compartida para todos los usuarios sin restricción alguna, esta red de datos puede recibir un ataque fácilmente y mucho más si se pensara realizar desde adentro, no existe un Firewall o equipo que haga sus veces, no existe un sistema de identificación y/o 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.

No se cuenta con unas políticas de seguridad que establezcan el uso de la red, sus servicios y equipamiento, los equipos de cómputo no cuentan con un sistema de protección contra software maligno, se encontraron puertos abiertos que pueden ser utilizados para robar, dañar, alterar la información que contienen los equipos de cómputo. Se puedo concluir de manera preocupante que el nivel de vulnerabilidad es de 10 sobre 10.

Se pudo concluir la necesidad urgente de tomar acciones correctivas o controles que permitan la reducción considerable de que se pueda producir un ataque por cualquiera de las vulnerabilidades identificadas.

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

Se recomienda la implementación de métodos de protección efectivos y actualizados que reduzcan el riesgo de ataque por software maligno y/o por intrusos.

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.

Una vez efectuado el proceso de aplicación de herramientas de pentesting sobre la red de datos del buque oceanográfico A.R. LIBERTAD, y presentado el informe con su respectivo análisis y recomendaciones, es evidente el descuido actual en cuanto a la seguridad

informática de dicha red se refiere, se puede evidenciar que no existe un solo método de seguridad implementado, por tanto la red de datos tiene el nivel de riesgo más alto que se le pueda asignar.

Igualmente se evidencia la presencia de programas maliciosos como son troyanos, virus y spyware, lo que pone en riesgo total la información valiosa que manejan los equipos de la red, la cual ya pudo incluso ser objeto de robo y/o alteración sin que a la fecha lo hayan notado.

Los directivos del buque oceanográfico A.R. LIBERTAD deben poner en consideración, todas las recomendaciones dadas con el fin de minimizar el riesgo a un ataque informático al cual está expuesta la red de datos y su más valioso que es la información y más la información obtenida en sus investigaciones oceanográficas, la cual es de gran trascendencia para Colombia y sus ciudadanos.

Nombre y apellidos de quien elaboró este RAE	Aydee Mercedes Viver Ramírez
Fecha en que se elaboró este RAE	24 de Abril de 2017