UNIVERSIDAD DE PAMPLONA FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES
PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR POR EL TITULO DE INGNIERO EN TELECOMUNICACIONES

TÍTULO:
GUIA METODOLOGICA PARA LA IMPLEMENTACION DE SOFTWARE SEGURO Y PROTOCOLOS DE SEGURIDAD EN SISTEMAS DE REDES DE DATOS

Autor:
LUIS CARLOS OZUNA MARTINEZ

Director:
Ing. ANGELO JOSEPH SOTO VERGEL

VILLA DEL ROSARIO- COLOMBIA
ABRIL de 2016

UNIVERSIDAD DE PAMPLONA FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES
PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR POR EL TITULO DE INGNIERO EN TELECOMUNICACIONES

TÍTULO:
GUIA METODOLOGICA PARA LA IMPLEMENTACION DE SOFTWARE SEGURO Y PROTOCOLOS DE SEGURIDAD EN SISTEMAS DE REDES DE DATOS

Autor:
LUIS CARLOS OZUNA MARTINEZ

Director:
Ing. ANGELO JOSEPH SOTO VERGEL

JURADO CALIFICADOR:

Ing. ANGELO JOSEPH SOTO VERGEL
M.Sc. JORGE ENRRIQUE HERRERA RUBIO
M.Sc. JOSE DEL CARMEN SANTIAGO GUEVARA

VILLA DEL ROSARIO- COLOMBIA
ABRIL de 2016

UNIVERSIDAD DE PAMPLONA FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES
PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO PRESENTADO PARA OPTAR POR EL TITULO DE INGENIERO EN TELECOMUNICACIONES

TEMA:

GUIA METODOLOGICA PARA LA IMPLEMENTACION DE SOFTWARE SEGURO Y PROTOCOLOS DE SEGURIDAD EN SISTEMAS DE REDES DE DATOS

FECHA DE INCIO DEL TRABAJO: NOVIEMBRE DE 2015
FECHA DE TERMINACION DEL TRABAJO: ABRIL DE 2016

NOMBRES Y FIRMAS DE AUTORIZACIÓN PARA LA SUSTENTACION

_____
LUIS CARLOS OZUNA MARTINEZ
AUTOR

_____ _____

ING. ANGELO JOSEPH SOTO
DIRECTOR

Esp. ADRIANA VILLAMIZAR P.
CORDINADOR DEL PROGRAMA

JURADO CALIFICADOR:

_____ _____

Ing. ANGELO JOSEPH SOTO V.

M.Sc. JORGE ENRIQUE HERRERA R.

_____
M.Sc. JOSE DEL CARMEN SANTIAGO G.

VILLA DEL ROSARIO N.S - COLOMBIA
MARZO DE 2016

DEDICATORIA

Dedico esta parte de mi proyecto de vida a Dios principalmente que me ha llenado de mucha fortaleza en todo momento y nunca me ha dejado desfallecer, a mi familia que me ha apoyado y acompañado durante todo el proceso de formación académica y personal orientándome y guiándome a cada instante.

Antonio Francisco Ozuna Ávila y Andrea Patricia Martínez Serpa, ustedes pareja ejemplar y modelo a seguir que, con su esfuerzo diario, su incansable lucha, su inmenso amor han sido los generadores y fundadores de este gran sueño.

A mis hermanos Álvaro José y Loly luz que siempre me han orientado y apoyado incondicionalmente con sus experiencias de vida, estado a cada instante en esos momentos difíciles, pero también buenos, gracias por ayudarme a cumplir esta meta.

A mis tías Yadira y Cecilia, ustedes al igual que toda la familia, mis tíos y primos con sus gestos de amor y cariño llevándome siempre por los buenos caminos.

AGRADECIMIENTOS

A Dios principalmente, a mi director de trabajo de grado Ángelo Joseph Soto, que ha estado constantemente apoyándome y orientándome en todo este proceso educativo.

También a todos los docentes, ingenieros, directores de programa, compañeros y amigos de estudio, que hicieron parte de mi formación académica y que trataron de transmitir sus enseñanzas de corazón al compartir todos sus conocimientos no solo académicos si no también experiencias personales, y que constantemente resaltaron el papel e importancia del ingeniero en telecomunicaciones para la comunidad y sociedad en general.

Agradezco a la universidad de pamplona en ambas sedes por recibirme como su hijo adoptivo durante un largo periodo de mi vida

RESUMEN

Para el desarrollo de este proyecto, se realizó una guía metodológica, orientada a la implementación de software seguro y protocolos de seguridad en los sistemas de redes de datos, para ello se analizarán tres metodologías existentes que son fundamentales, reconocidas y avaladas por organismos internacionales, todas estas metodologías serán orientadas y enmarcadas en el estudio de los sistemas de redes WAN, con el fin de verificar fallas de seguridad.

La metodología OSSTMM, está encaminada a realizar pruebas y análisis de seguridad, desarrollada por la organización ISECOM, el Instituto para la Seguridad y las Metodologías Abiertas, que es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet [1]. La siguiente metodología que será elemento de la investigación es la ISSAF, esta metodología está compuesta por una estructura de análisis de seguridad en varios dominios y detalles específicos de test o pruebas para cada uno de estos. Su objetivo es proporcionar procedimientos muy detallados para el testing de sistemas de información que reflejan situaciones reales [2]. Finalmente, en cuanto a metodologías se refiere, la OWASP hace énfasis en la seguridad de auditoría web, abierta y colaborativa, orientada al análisis de seguridad de aplicaciones Web, y usada como referente en auditorías de seguridad, para objeto de análisis se usará y categorizará el top 10 de vulnerabilidades existentes en la actualidad en aplicaciones web [3].

La guía metodológica incluye componentes del estándar ISO/IEC, realizando un estudio detallado de las normas ISO/IEC- 27000, 27001, 27002 que son uno de los estándares que garantiza mediante un conjunto de procedimientos e instrucciones de cómo se debe implementar un sistema de gestión de la seguridad de la información [4]. También Se tomarán como referencia Comman Criteria (Criterios comunes) que van a permitir tener un panorama mucho más detallado de todos los requerimientos a los cuales debe acogerse el desarrollador de software para mantener los perfiles y estándares de calidad y seguridad que el entorno actual requiere, apoyado bajo componentes del estándar ISO / IEC 15408 [5].

Así mismo se determinaron los componentes y las tecnologías que actualmente utiliza una red WAN, con el fin de analizar y determinar mediante mediciones de campo, los agujeros de seguridad que existen en estas redes, posteriormente se realizaron algunas pruebas de campo con el donde se analizó la vulnerabilidad de algunas aplicaciones web de universidades de la región como la UIS, UPA, UFPS y UDESCON, todo esto con la ayuda del sistema operativo KALI LINUX y a su vez los software OPENVAS y OWASP-ZAP, lo cual permitió el desarrollo de una guía teniendo en cuenta factores, metodologías y estándares anteriormente mencionados.

ABSTRACT

For the development of this project, a methodological guide aimed at implementing secure software and security protocols in network systems data for this three existing methodologies that are fundamental, recognized and endorsed by international organizations will be analyzed was performed, all these methodologies are oriented and framed in the study of systems WAN networks to verify security flaws.

The OSSTMM methodology, is aimed at testing and safety analysis, developed by the ISECOM organization, the Institute for Security and Open Methodologies, which is one of the most complete professional standards and commonly used in Security Audits to check Security Systems from the Internet [1]. The following methodology will be element of the research is the ISSAF, this methodology consists of a structure of security analysis in multiple domains and specific details of test or tests for each of these. It aims to provide very detailed procedures for the testing of information systems that reflect real situations [2]. Finally, in methodologies it is concerned, the OWASP emphasizes web security audit, open and collaborative, oriented security analysis Web applications, and used as a benchmark in security audits for scope of analysis used and categorize the top 10 currently existing vulnerabilities in web applications [3].

The methodological guide includes components of ISO / IEC standard, making a detailed study of the ISO / IEC-27000, 27001, 27002 standards are one of the standards guaranteed by a set of procedures and instructions of how to implement a system management information security [4]. They should also be taken as a reference common Criteria (Common Criteria) that will allow to have a much more detailed analysis of all requirements panorama to which the software developer must be upheld to maintain profiles and standards of quality and safety that the current environment requires, supported standard components under ISO / IEC 15408 [5].

Likewise, the components and technologies that currently use a WAN, in order to analyze and determine by field measurements, security holes that exist in these networks, then some field tests were conducted with where it determined was analyzed the vulnerability of some web applications from universities in the region as the UIS, UPA, UFPS and UDES, all with the help of Kali Linux operating system and turn Omesar and OWASP-ZAP software, which allowed the development of a guide taking into account factors, methodologies and standards mentioned above

CONTENIDO

LISTA DE TABLAS

LISTA DE GRÁFICAS

LISTA DE FIGURAS

GLOSARIO

Amenaza: es la probabilidad de ocurrencia de un suceso potencialmente desastroso durante cierto periodo de tiempo, en un sitio dado.

Vulnerabilidad: Es el grado de pérdida de un elemento o grupo de elementos bajo riesgo, resultado de la probable ocurrencia de un suceso desastroso expresada en una escala

Ciclo De Vida: Del Desarrollo Del Software: Son las tareas básicas que permiten desarrollar software de calidad desde el primer instante del propio proyecto.

Escaneo De Puertos: se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un cortafuegos

Protocolo: conjunto de reglas y estándares que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red, como teléfonos o computadoras

Agujero De Seguridad es el fallo de un programa que permite mediante su explotación violar la seguridad informática de un sistema.

Capítulo 1

1. Introducción

Las tecnologías de la información y las comunicaciones desde hace algunos años han venido siendo parte de nuestra vida diaria, y hemos sido testigos de su enorme crecimiento, estos avances han generado una mejor calidad de vida a ciertas comunidades y han facilitado muchísimo procesos internos y externos de organizaciones estatales y privadas permitiéndoles así brindar un mejor servicio a la sociedad, pero también ahorrando en mayor medida dinero y tiempo.
Debido a este desarrollo tecnológico, han surgido muchas normas y estándares de seguridad que indican a estas entidades como deben ser los procesos para la implementación y protección de sus datos, emitiendo así una certificación que describa y que acredite los buenos procedimientos de dicha organización, pero esta certificación es un tanto costosa para las entidades

Estándares de la ISO/IEC como la serie 27000, metodologías como la OWASP, ISAAF Y OSSTMM, en sus versiones anteriores, las cuales las podemos adquirir de manera gratuita y ejecutarlas como método educativo y por qué no a niveles empresariales, (respetando los derechos de autor y demás), nos ofrecen en gran medida un conjunto de procesos y métodos de ejecución, así mismo una guía de pruebas que posibilitan qué usuarios con ciertos conocimientos las apliquen.

Este documento contiene en el capítulo 2 un resumen sustancioso de los estándares ISO/IEC 27000, 27001 y 27002, así mismo el estándar ISO/IEC 15408 que se hace énfasis a los criterios comunes en los procesos de desarrollo de software, también se mencionan componentes de una red WAN y su aplicación.

En el capítulo 3 encontramos una descripción de las metodologías OWASP, ISSAF, OSSTMM, y referenciando las fases de desarrollo y detallando algunas de ellas. en el capítulo 4 se realizan unas pruebas de vulnerabilidad a las aplicaciones web de algunas universidades de la región y se obtienen resultados expuestos estadísticamente en gráficas, pero además se categoriza la vulnerabilidad más común en el top 10 de la metodología OWASP, en el capítulo 5 se describen las herramientas o algoritmos que permiten la detección de vulnerabilidades, en el capítulo 6 se detallan los escenarios de vulnerabilidad, todo esto se desarrollará para posteriormente el capítulo 7 tomar como referencias estas metodologías y procesos descritos en los capítulos anteriores y proponer una metodología propia que integra y especifica los requerimientos para la implementación de software y protocolos de seguridad en sistemas de redes de datos

1.1 Planteamiento del Problema

Desde hace algunos años los sistemas de redes de datos han sido objeto de vulnerabilidades, causando perdida de información y permitiendo que agentes no autorizados cuenten con acceso a información confidencial, un ejemplo de ello es que a nivel mundial la detección de malware creció en un 40% en el primer trimestre del año en curso [6].

Uno de los factores más importantes que inciden en esta problemática, es la garantía en la seguridad de datos confidenciales. Estudios realizados en agosto de 2014 arrojan que Latinoamérica cerca del 41% de las empresas encuestadas dijeron haber sufrido una infección con malware, en cuanto a Phishing que es otra de las vulnerabilidades más comunes, afectó al 17% de las empresas encuestadas en esta misma región. En el caso de Colombia se observa que no es ajena a esta problemática ya que cerca del 34% de empresas han tenido contacto con algún tipo de código malicioso o malware [7].

Una encuesta realizada por la ACIS (Asociación Colombiana De ingenieros de Sistemas), y expuesta en la XIII jornada internacional de seguridad informática, Ciber-Seguridad y Ciber-Defensa, realizada en el año 2013 , indican que en Colombia se presentaron diferentes tipos de ataques como: Acceso no autorizado a la web, con un 32,1%, Software no autorizado con 55,56%, Phishing 17,9% entre otros ataques, este estudio también indica que este tipo de ataques, tendió a Incrementarse en un 8,66% frente al año anterior, Por otro lado encontramos un incremento del 6,18% de entidades que manifiestan la presencia de entre 4 y 7 incidentes que se han presentados en sus organizaciones [8].

Empresas manifiestan que la falta de implementación de un antivirus, firewall y otro tipo de software, no es suficiente para estar a salvo de diversos ataques presentes en el medio, y más cuando no existen políticas de seguridad e implementación de software seguro en los sistemas de redes de datos. [9]

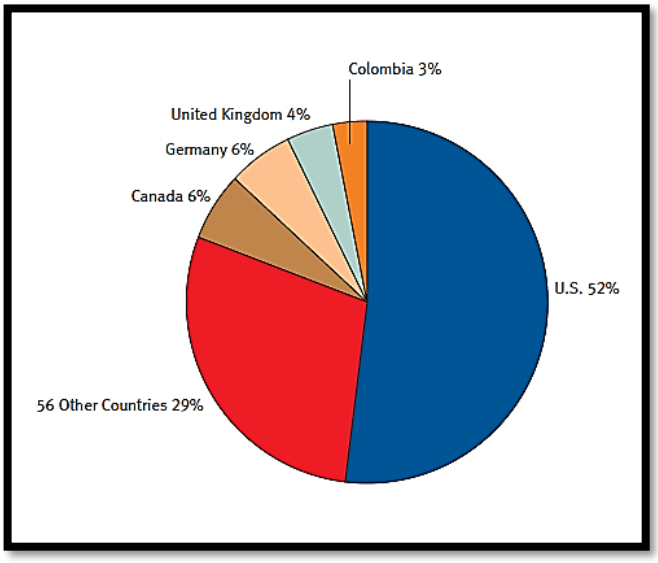
De acuerdo con todas las estadísticas y argumentos expuestos, se observa claramente que existe un déficit o fallo en la seguridad de entidades u organizaciones, en muchos casos por desconocimiento o falencias en los procesos y requisitos mínimos de protección y defensa, formando parte del gran porcentaje de inseguridad informática que se vive hoy en día

1.2 Justificación

Las tecnologías de la información nos ofrecen un sin número de herramientas, una de estas es la conexión a la red, integrando algún tipo de software. Así mismo las Tics son uno de los pilares fundamentales con los que cuenta una organización, permitiéndole aplicar métodos de protección que posteriormente traerán beneficios como credibilidad y confiabilidad por parte de usuarios que de una u otra forma tienen algún contacto con este medio, y que cuentan con un mundo de posibilidades de acceso a la información, pero de la misma manera este contacto genera una exposición a nuevos riesgos que involucran factores de seguridad.

Por tanto, la seguridad de la información para las organizaciones, es un tema que desde sus inicios se ha visto con una perspectiva compleja y difícil de adoptar, pero la causa principal de esta situación se refleja en estudios realizados, determinando que la complejidad de los flujos de información, son el obstáculo más importante cuando se habla de protección o permeabilidad de la información dentro de las empresas. En el año 2013 hubo un incremento en el 16,03% de los encuestados que consideran que dicha situación, hace difícil los procesos de adopción, e implementación de la seguridad de la información dentro de las organizaciones [8].

Los ataques informáticos son a menudo una de las causas de pérdida o suplantación de información, uno de estos ataques es el phishing que para EE. UU, representan el 52%, seguido por Canadá, Alemania, el Reino Unido y Colombia con un 3%, todo esto en referencia a nivel mundial.



Grafica 1. Ataques de Phishing a nivel mundial, según EMC [10]

Estudios realizados por diferentes organizaciones en Colombia, determinan y concluyen que se deben realizar esfuerzos mayores por construir modelos de seguridad de la información que permitan una forma de defensa ante las amenazas existentes en la actualidad y sugieren recordar que los enemigos informáticos están cada día más organizados, también exponen que la seguridad de la información penetra día a día en los sectores económicos del país, mostrando su importancia como elemento de apoyo estratégico a la consecución de los objetivos de las organizaciones [8].

Partiendo de lo anterior, se evidencia que los métodos y controles propios de las empresas para establecer y analizar los componentes activos de información, ha dejado de ser algo que se le asigne al técnico en seguridad, para evolucionar en una disciplina que es necesaria para las entidades. considerando todo esto, el desarrollo de una guía metodológica orientada a la problemática de software seguro en sistemas de redes de datos, permite que no solo entidades sino, también en la implementación de proyectos por muy pequeños que se consideren, apliquen un plan de contingencia asociado a las vulnerabilidades existentes en el medio, generando así un mayor grado de confiabilidad y mejor desempeño en los procesos. La guía metodológica también va a darle la posibilidad a aquellas pequeñas y medianas empresas u organizaciones, que no cuenten con un amplio capital para destinarlo a las certificaciones de seguridad de tipo internacional, tener una defensa previa ante las posibilidades de riesgo informático, contando así con una metodología confiable al momento de hacer una implementación de software seguro en los diferentes sistemas de redes de datos con los que cuenten dichas entidades.

1.3 Delimitación

1.3.1 Objetivo General

Elaborar una guía metodológica para la implementación de software seguro y protocolos de seguridad en sistemas de redes de datos

1.3.2 Objetivos Específicos

- Identificar los requerimientos de un sistema de red que le permitan cumplir con normas y estándares de seguridad.
- Clasificar, basado en datos estadísticos, mediante mediciones de campo, los procesos para el desarrollo de software seguro según su nivel de efectividad.
- Determinar cuáles son las herramientas y algoritmos existentes que permiten la detección de las amenazas y vulnerabilidades.
- Proponer una guía metodológica y de buenas prácticas de cómo implementar software de manera que apoye y respalde la seguridad de la información en los sistemas de redes de datos.

1.3.3 Acotaciones

- Se realizará el desarrollo de la guía metodológica, enfocándonos en las redes de área metropolitana (WAN) basándonos en las tecnologías y protocolos de comunicación que esta utilice.
- La recolección de la información se realizará en un intervalo de tiempo de 5 años, desde el año 2010 hasta el presente año.
- La información fundamental de esta monografía, Será tomada de Tesis y proyectos de grado, tanto en el área de pregrado como postgrado, de diversos repositorios de universidades y otras fuentes de información.
- Se utilizarán herramientas de medición, gratuitas como OPENVAS de kali Linux, que ayuden a la comparación de vulnerabilidades, permitiendo así realizar una propuesta detallada

1.4. Marco Teórico

1.4.1 Ingeniería de Software Seguro

Es una disciplina de la ingeniería del software que busca proporcionar garantías objetivas respecto a la seguridad del software producido. Para ello se aplican mecanismos y se producen evidencias durante el proceso (medibles, verificables, y repetibles), que garantizan que el software exhibe de manera consistente las propiedades de seguridad que se le requieran. En particular, y partiendo del axioma "la seguridad absoluta no es alcanzable", el software seguro es capaz de resistir la mayoría de los ataques, tolerar aquellos que no pueda resistir, y recuperarse rápidamente y con el menor impacto de aquellos ataques que no pueda tolerar [11]

1.4.2 Metodología OSSTMM

Según (*R. Alder, J. Burke, C. Keefer, A. Orebaugh, L. Pesce, and E. S. Seagren, How to Cheat at Configuring Open Source Security Tools, 2010)*, el manual de la metodología abierta de comprobación de seguridad (open source security testing methodology manual), representa uno de los estándares profesionales más completos para analizar la seguridad de los sistemas. Describe minuciosamente, las fases que habría que realizar para la ejecución de la auditoría. Se ha obtenido mediante un consenso entre más de 150 expertos internacionales sobre el tema. Se encuentra en constante expansión gracias a la colaboración incansable de los analistas expertos de seguridad que aportan sugerencias y experiencias sobre el manual de la metodología abierta [12].

Para La OSSTMM se focaliza en los detalles técnicos de exactamente qué elementos deben ser probados, que hacer antes, durante y después de una prueba de seguridad; así como medir los resultados. Nuevas pruebas provenientes de mejores practica internacionales, leyes, regulación y asuntos éticos son regularmente añadidas y actualizadas [13]

1.4.3 Metodología ISSAF

(*Diego Camacho Moreno, Evaluaciones de Seguridad en entornos TIC*, 2013), expone que la metodología ISSAF, es un marco estructurado del *Open Information System Security Group*, que categoriza las evaluaciones de seguridad de sistemas de información en varios dominios y detalla criterios de prueba específicos por cada uno de ellos. Este marco debe ser usado para cumplir con los requerimientos de

evaluación de la seguridad de una organización, y opcionalmente ser usado como referencia para cumplir con otras necesidades dentro del campo de la seguridad de la información. Incluye la faceta critica de los procesos de seguridad, su evaluación y reforzado para obtener una imagen global de las vulnerabilidades que pueden existir [13]

1.4.4 Metodología OWASP

De acuerdo con (Erdogan, G Meland, PH Mathieson, Security testing in agile web application development-a case study using the east methodology, 2010), la metodología OWASP (open web aplicattion security project) la cual está diseñada como un marco de trabajo que ayude en el proceso del ciclo de desarrollo de software (SDLC), esta promueve una solución flexible que mejora el proceso de desarrollo, teniendo en cuenta el inicio de la seguridad en la ingeniería de software, estructuralmente esta metodología consta de las siguientes fases: [15].

Fase 1: Antes de Empezar el desarrollo.
Fase 2: Durante el diseño y la definición.
Fase 3: Durante el desarrollo.
Fase 4: Durante la implementación.
Fase 5: Mantenimiento y operaciones

1.4.5 Sistemas de Redes de Datos

Un sistema de redes de datos, consiste en una infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino, y con base en esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones En lo sucesivo se denominará "red de telecomunicaciones" a la infraestructura encargada del transporte de la información. Para recibir un servicio de telecomunicaciones, un usuario utiliza un equipo terminal a través del cual obtiene entrada a la red por medio de un canal de acceso. Cada servicio de telecomunicaciones tiene distintas características, puede utilizar diferentes redes de transporte, y, por tanto, el usuario requiere de distintos equipos terminales [16].

1.4.5.1 LAN

Cuando el ámbito se reduce a un edificio o incluso campus o recinto. Se caracterizan por tener velocidad de transmisión elevada, entre 10 Mbits y 1 Gbits o mayores; una tasa de error de transmisión despreciable y los recursos y el mantenimiento de la red son por cuenta del propietario [17].

1.4.5.2 Redes WAN

Cuando una empresa crece y agrega sucursales, servicios de comercio electrónico u operaciones globales, una sola red LAN ya no es suficiente para satisfacer los requisitos de la empresa. En la actualidad, el acceso a una red de área extensa (WAN, Wide Area Network) se ha vuelto esencial para las empresas grandes.
Existe una variedad de tecnologías WAN que satisfacen las diferentes necesidades de las empresas y hay muchas maneras de agrandar la red. Al agregar el acceso WAN, se presentan otros aspectos a tomar en cuenta, como la seguridad de la red y la administración de las direcciones. Por lo tanto, el diseño de una WAN y la elección de los servicios de red adecuados de una portadora no es una cuestión simple. Las tecnologías LAN proporcionan velocidad y rentabilidad para la transmisión de datos dentro de organizaciones, a través de áreas geográficas relativamente pequeñas [18].

1.4.6 Aplicación Web

Las aplicaciones web reciben este nombre porque se ejecutan en la internet. Es decir que los datos o los archivos en los que trabajas son procesados y almacenados dentro de la web. Estas aplicaciones, por lo general, no necesitan ser instaladas en tu computador.
El concepto de aplicaciones web está relacionado con el almacenamiento en la nube. Toda la información se guarda de forma permanente en grandes servidores de internet y nos envían a nuestros dispositivos o equipos los datos que requerimos en ese momento, quedando una copia temporal dentro de nuestro equipo. En cualquier momento, lugar y desde cualquier dispositivo podemos acceder a este servicio, sólo necesitamos una conexión a internet y nuestros datos de acceso, que por lo general son el nombre de usuario y contraseña. Estos grandes servidores de internet que prestan el servicio de alojamiento están ubicados alrededor de todo el mundo, así hacen que el servicio prestado no sea tan costoso o gratuito en la mayoría de los casos y extremadamente seguro [19]

1.4.7 Firewall

Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.
Un firewall puede ayudar a impedir que hackers o software malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de Internet. Un firewall también puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos.[20]

1.5 Estado del Arte

Luego de que apareciera el concepto de seguridad informática, años después se empezó a hablar de desarrollo software, pero no se tenían en cuenta aspectos importantes como la seguridad y calidad en éste, generando así muchas alteraciones en los procesos de perfeccionamiento tales como la planificación, estructura y control. A raíz de esas malas prácticas, se han desencadenado una serie de vulnerabilidades causando así una perdida gigantesca de dinero llegando a la suma de alrededor de 6,6 millones de dólares [21].

En el transcurso de los años se han implementado PKI (*Public Key Infrastructure*), y actualmente son utilizadas en diversas aplicaciones como: Identificación de servidores, Autenticación y autorización para aplicaciones web, Firma digital de documentos, Autenticación de VPN, Correo electrónico firmado y cifrado, Mensajería instantánea segura, Seguridad de la red inalámbrica, entre otras [22].
A nivel internacional y para (*E. R. Trujillo Machado, "Diseño e implementación de una VPN en una empresa comercializadora utilizando IPSEC, 2011*), que en su estudio realizo una integración de una PKI con un IPSec, como respuesta a la necesidad para autenticar de forma fiable un conjunto de nodos que desean comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso. Define que la existencia de una PKI ofrece ventajas, ya que centraliza el alta y baja de los usuarios. Además, posibilita la integración de tarjetas inteligentes, para soportar certificados, lo cual resulta muy interesante en un entorno de tele-trabajadores o usuarios móviles [23].
Por otro lado, también a nivel internacional un estudio realizado por (*F. López Provencio, "Desarrollo dirigido por la seguridad, 2015*), en donde realiza una comparativa entre las metodologías de desarrollo de software seguro existentes, como OSSTMM OWASP componentes de ISSAF y posteriormente realiza una comparativa, definiendo varios aspectos como: Metodología de Trabajo, Métrica de la seguridad del sistema, lista de vulnerabilidades en el código, entre otras. [24]
En la investigación realizada por (*Gaston Alejandro Toth, implementación de una guía NIST SP 800-30 mediante la utilización de OSSTMM, 2014*), en donde logra desarrollar una metodología de análisis de riesgos basada en el estándar NIST SP 80030 en el cual las distintas fases sean implementadas por la metodología OSSTMM y sugiere que, en el caso del desarrollo de software, la seguridad debe formar parte del diseño y debe ser implementada durante todo el proceso. Por otra parte, la gente que se encarga de administrar los sistemas y las redes de datos debe ocuparse de mantener los servidores actualizados, así como también definir diversas políticas que lleven a un ambiente más protegido. El personal que no pertenece al área de informática debe ser capacitado para cumplir con las políticas implementadas, ya que no sólo es importante la información que circula por la red, sino que los documentos escritos o respuestas verbales pueden dar lugar al compromiso del sistema o a una violación de la confidencialidad de los datos [25].

En el caso nacional se desarrolló una propuesta metodológica propuesta por (*Mendoza, Martha Ascencio y Moreno Patiño, Pedro Julián, Desarrollo de una propuesta metodológica para determinar la seguridad en una aplicación web*), que tiene como objetivo determinar la seguridad en una aplicación web puede ser de gran utilidad. La propuesta metodológica incluye componentes del estándar ISO 27001 y de metodologías existentes, tales como OWASP e ISSAF. Para hablar de seguridad de la información, no sé puede dejar de hablar de ISO 27001, debido a que es el estándar de facto para la seguridad en la información, que ofrece un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejoras de todos los procesos que involucran la seguridad de la información en una organización por medio del Sistema de Gestión de la Seguridad de la Información (SGSI). OWASP es una metodología que tiene en cuenta la seguridad en el ciclo de desarrollo del software (SDLC). Por otro lado, ISSAF es una metodología para pruebas de intrusión en un sistema informático [26]

Capítulo 2

2. Normas, Estándares de Seguridad y Componentes Funcionales de la WAN

2.1 Serie ISO/IEC 27000

El conjunto de normas y estándares ISO/IEC 2700 son el fruto de muchos años de trabajo, de recopilación y evolución de anteriores normas de la ISO (*International Organization for Standarization*) e IEC (International Electrotechnical Commission), las cuales se enfocan en facilitar y proporcionar un marco de gestión de la seguridad de la información que puede ser implentada y utilizada en organizaciones de cualquier tipo sean privadas o públicas. Y de cualquier tamaño, grandes o pequeñas. Estos conjuntos de normas internacionales muestran un panorama e ilustran de manera general el SGSI (*sistema de seguridad de la información*) soportado bajo el título general de tecnología de la información - Técnicas de seguridad

Figura 1. Estructura General Norma Iso/Iec 27000

2.2 ISO/IEC 27001

El estudio de esta norma hace referencia a todas las regulaciones internacionales en las tecnologías de la información, técnicas de seguridad, sistemas de gestión de seguridad de la información y sus requerimientos. Esta norma ha sido un modelo para establecer, implementar, operar, revisar, mantener y mejorar los sistemas de

gestión de seguridad (SGSI), cabe destacar que estos requerimientos que van a ser expuestos más adelantes, marcharan conjuntamente al cambio en las tecnologías de la información y las comunicaciones puesto que a medida que se incorporen más o diferentes tecnologías posteriormente y de la mano a esta evolución se tendrá que regular internacionalmente como lo ha venido haciendo la ISO/IEC. Varios de los componentes incluidos en esta norma se detallarán a continuación de la siguiente manera:

Alcance: El alcance es de suprema importancia para cualquier organización ya que se debe tener muy claro cuáles serán los activos que va a proteger y cuáles no, antes de decidir la protección más adecuada.

Se debe categorizar y definir las fortalezas de seguridad de la entidad y que fracciones de la información quedaran expuestas, esto significa que no se debe aceptar que ningún sistema de información, unidad o dispositivo quede a ambos lados ya que sería el eslabón más débil y podría afectar de manera significativa la información de la organización.

SGSI: La evaluación de los sistemas de gestión de la seguridad de la información es un paso critico; cualquier control o monitoreo implementado antes de haber realizado la evaluación, poder resultar deficiente e inapropiado. En algunos casos esta inspección, luego de ser puesta en marcha resulta ser demasiado robusta y por consiguiente no será tan efectiva como se espera.

Evaluación del Desempeño: Se encarga de medir la efectividad, comportamiento y desempeño del SGSI, realizando auditorías internas y revisiones del mismo, considerando cuando se deben realizar estas evaluaciones y definir quién debe realizar la tarea de recolectar la información [4]

En la siguiente grafica se muestra la estructura general de la norma ISO/IEC 27001 y del SGSI

Figura 2 Estructura General Norma Iso/Iec 27001[27]

2.3 ISO/IEC 27002

Al igual que la norma anteriormente mencionada en su contenido existen múltiples aspectos que tratan, pero ya relacionando u orientándolo hacia las Técnicas de seguridad y Código de prácticas para los controles de seguridad de la información.

Políticas Seguridad: Están basadas en el contexto en el que opera una organización considerando las metas y objetivos que son adoptadas en la entidad. Existen una serie de procedimientos en los cuales esta norma específica de cómo se deben realizar u organizar las políticas de seguridad, resaltándolo de la siguiente manera:

1. Políticas
2. Introduccion
3. Ámbito de la aplicación
4. Objetivos
5. Principios
6. Responsabilidades
7. Resultados clave
8. Políticas relacionadas

Organización: Establece la administración de la seguridad de la información, haciéndola parte esencial para el cumplimiento de los objetivos y las actividades de la entidad, aquí se efectúan labores tales como la aceptación de las políticas de seguridad, la coordinación de la implementación de la seguridad y la asignación de funciones y responsabilidades como lo son:

1. Organización interna
2. Dispositivos para movilidad y teletrabajo

Seguridad: Tiene como finalidad la de instruir, formar y educar de manera continua al personal de una organización desde el momento de ingresar, y prepararlo para enfrentar cualquier situación u actividad relacionada con las medidas de seguridad que afectan continuamente el desarrollo de sus funciones y de las metas depositadas en asuntos de confidencialidad. También se tienen en cuenta otros aspectos como:

1. Antes de la contratación
2. Durante la contratación
3. Cese o cambio de puesto de trabajo

Gestión Activos: La parte fundamental de este dominio se centra en que todos los integrantes de la organización tengan un amplio conocimiento sobre los activos que posee, como parte fundamental en la administración de riesgos. Estos activos deben ser categorizados y clasificados de acuerdo a la criticidad y sensibilidad de la información, teniendo siempre presente de su funcionalidad y se clasificaran de la siguiente forma:[28]

- **Recursos de información:** bases de datos, documentación.

- **Recursos de software:** software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

- **Activos Físicos**: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos, switches de datos, etc

- **Servicios**: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

2.4 ISO/IEC 15408 (CC)

La norma ISO / IEC 15408 Common Criteria para la evaluación de la tecnología de la información regula la evaluación objetiva, repetible y comparable de las propiedades de seguridad de productos y sistemas de información. Generando una declaración de seguridad del producto o sistema evaluado verdadera, la cual procede de una evaluación rigurosa y satisfactoria, generando un alto grado de confianza [29].

2.4.1 Destinatarios de los CC

Existen tres grupos con un interés general por la evaluación de las propiedades de seguridad de los productos o sistemas de TI: usuarios, fabricantes y evaluadores. Los criterios presentados en la norma han sido diseñados para apoyar las necesidades de estos tres grupos:

Usuarios. Para asegurar que la evaluación satisface sus necesidades al éste el objetivo fundamental y la justificación del proceso de evaluación.

Fabricantes. La norma pensada para apoyarlos en los procesos de evaluación de sus productos o sistemas y en la identificación de requisitos de seguridad que deben ser satisfechos por cada uno de dichos productos o sistemas.

Evaluadores. La norma contiene criterios para que los evaluadores emitan veredictos sobre la conformidad del objeto evaluador (TOE) con sus requisitos de seguridad. Aunque los CC no especifican procedimientos a seguir para realizar estas acciones. • Otros. Oficiales de seguridad, Auditores, Diseñadores de arquitecturas de seguridad, Autoridades de acreditación, Patrocinadores de evaluación y Autoridades de evaluación.

3. Componentes Funcionales Red WAN

se trata de los elementos de red que interconectan las redes de área local (LAN). La WAN proporciona acceso a computadoras, servidores de archivos y servicios ubicados en lugares distantes. A medida que la empresa crece y ocupa más de un sitio, es necesario interconectar las LANs de las sucursales con la casa central, para formar una red de área amplia. En la actualidad, existen muchas opciones para implementar soluciones WAN, que difieren en tecnología, velocidad y costo. Estar familiarizados con estas tecnologías permite conocer el diseño y la evaluación de la red. [30].

3.1 Requerimientos Funcionales del Sistema de Red WAN

Teniendo en cuenta las características de este tipo de red y para determinar los requerimientos funcionales de una red WAN, se hace necesario tener en cuenta componentes de diseño e instalación. Dentro de los requerimientos funcionales que debe tener una red WAN para su comunicación tenemos:

- Topologías de red.
- Control de Acceso a la red
- Medios de transmisión
- Protocolos
- Elementos de interconexión

3.1.1 Topologías de Red.

La manera de interconectar los distintos elementos de una red determina el comportamiento de ésta. Aunque, su eficiencia y aprovechamiento dependerá también de los protocolos de comunicación que se utilicen. Según la topología elegida, la red va a estar condicionada por:

- La mayor o menor flexibilidad de la red para añadir o quitar nuevos nodos.

- La repercusión que en el comportamiento de la red pueda tener el fallo de un nodo.

- El flujo de información que pueda transitar por la red sin que se produzcan interferencias ni retrasos. Las múltiples configuraciones que puedan presentarse obedecen básicamente a tres tipos:

Punto a Punto: En esta topología cada nodo se conecta a otro a través de circuitos dedicados, es decir, canales que son arrendados por empresas o instituciones a las compañías telefónicas. Dichos canales están siempre disponibles para la comunicación entre los dos puntos. Esta configuración es solo funcional para pequeñas WANs ya que todos los nodos deben participar en el tráfico, es decir que si aumenta la cantidad de nodos aumenta la cantidad de tráfico y esto con el consiguiente encarecimiento de la red.

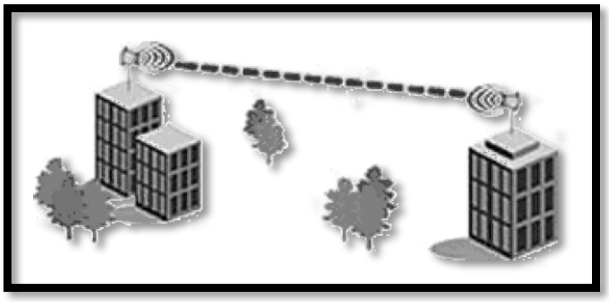


Figura 3. Topología punto a punto.

Estrella: En una red en estrella todas las estaciones se comunican entre sí a través de un dispositivo central. Éste asume todas las transferencias de información que se realicen en la red, así como las tareas de control. Además, posee todos los recursos comunes de la red.

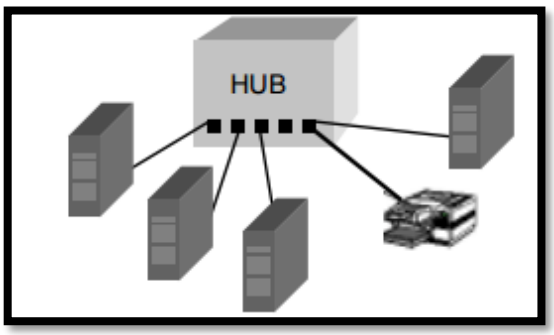


Figura 4. Topologia en Estrella.

Anillo: Los nodos de la red están conectados formando un anillo de forma que cada estación tiene conexiones con otras dos. Los mensajes viajan por el anillo de nodo en nodo y en una única dirección, de manera que todas las informaciones pasan por todos los módulos de comunicación de las estaciones. Cada nodo reconoce los mensajes a él dirigidos y retransmite los mensajes que se dirigen a otra estación. El control de la red puede ser centralizado o distribuido entre varios nodos.

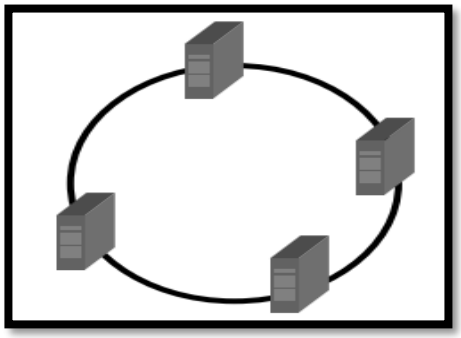


Figura 5. Topologia en Anillo

Malla: En esta topología la esencia es buscar la interconexión de los nodos de tal manera que si uno falla los demás puedan redireccionar los datos rápida y fácilmente. Esta topología es la que más tolerancia tiene a los fallos porque es la que provee más caminos por donde puedan viajar los datos que van de un punto a otro [31].

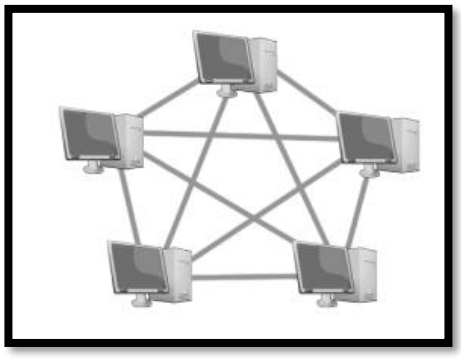


Figura 6. Topologia en Malla [31]

3.1.2 Control de Acceso a la Red

El control de acceso a la red. Una WAN puede implementarse según diversas topologías. Para todas ellas es necesario establecer mecanismos para gestionar la información que se transmite por el medio de comunicación. El control de acceso a la red puede clasificarse en:

Centralizado: Una estación maestra controla el acceso a la red de las estaciones esclavas mediante sondeo (polling). La estación maestra invita a transmitir a cada estación esclava según la tabla de secuencias de sondeo.

Distribuido: Las estaciones en un bus de paso de testigo son maestras temporalmente mientras mantienen el testigo (token). Cuando una estación quiere transmitir, lo que hace es esperar a que el testigo vacío pase por ella. En este instante introduce la información en el testigo y lo transmite. El testigo circula por la red hasta llegar a su destino, el cual, hace copia de la información transmitida e introduce una señal de información recibida. Cuando el token llegue a la estación emisora, liberará el testigo y otra estación podrá transmitir.

Descentralizado: Todas las estaciones se encuentran en contienda por un medio en base de igualdad (CSMA/CD - Carrier Sense Multiple Access / Collision Detect). Cuando una estación quiere transmitir, escucha el medio y si está vacío transmite, sino espera un tiempo aleatorio y lo vuelve a intentar (CSMA). En el caso de transmitir, la estación sigue escuchando al medio, si detecta colisión, aborta la transmisión y espera un tiempo aleatorio y vuelve a intentarlo (CD).

3.1.3 Medios de Transmisión

Microondas: Microondas o también llamadas ondas de radio que van de una antena parabólica a otra, sirven para comunicaciones de vídeo o telefónicas. La movilidad que pueden caracterizar estos equipos y el ahorro económico que produce el hecho de no tender cable a cada sitio en que quiera enviarse o recibir la información es una de las más usadas para comunicaciones móviles. Uno de los inconvenientes es que son afectadas por el estado del clima.

Comunicación por satélite: Los satélites de comunicación son repetidores de microondas localizados en el cielo. Están constituidos por uno o más dispositivos recepto-transmisores, cada uno de los cuales capta y re-transmite la señal de microondas. El flujo dirigido hacia abajo puede ser muy amplio y cubrir una parte significativa de la superficie de la tierra, o bien puede ser estrecho y cubrir un área de cientos de kilómetros de diámetro. Los satélites de comunicación tienen varias propiedades que son diferentes de las que presentan los enlaces terrestres punto a punto.

Fibra óptica: La fibra óptica es un conductor de ondas en forma de filamento, generalmente de vidrio, también puede ser de materiales plásticos. Dirigen la luz a lo largo de su longitud usando la reflexión total interna. Normalmente la luz es emitida por un láser o un LED. Las fibras son ampliamente utilizadas en telecomunicaciones, ya que permiten enviar gran cantidad de datos a gran velocidad, mayor que las comunicaciones de radio y cable.

3.1.4 Protocolos

3.1.4.1 Protocolos Capa Física WAN

Describen cómo proporcionar conexiones eléctricas, mecánicas, operacionales, y funcionales para los servicios de una red de área amplia. Estos servicios se obtienen en la mayoría de los casos de proveedores de servicio WAN tales como las compañías telefónicas, portadoras alternas, y agencias de Correo, Teléfono, y Telégrafo (PTT: Post, Telephone and Telegraph).
La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de conexión de los datos (DCE). Típicamente, el DCE es el proveedor de servicio, y el DTE es el dispositivo asociado. En este modelo, los servicios ofrecidos al DTE se hacen disponibles a través de un módem o unidad de servicio del canal/unidad de servicios de datos (CSU / DSU). Algunos estándares de la capa física que especifican esta interfaz son:

- **EIA/TIA-232D:** Esta norma fue definida como una interfaz estándar para conectar un DTE a un DCE.

- **EIA/TIA-449:** Junto a la 422 y 423 forman la norma para transmisión en serie que extienden las distancias y velocidades de transmisión más allá de la norma 232.

- **V.35**: Según su definición original, serviría para conectar un DTE a un DCE síncrono de banda ancha (analógico) que operara en el intervalo de 48 a 168 kbps.

- **X.21**: Estándar CCITT para redes de conmutación de circuitos. Conecta un DTE al DCE de una red de datos pública.

- **G.703**: Recomendaciones del ITU-T, antiguamente CCITT, relativas a los aspectos generales de una interfaz.

- **EIA-530**: Presenta el mismo conjunto de señales que la EIA-232D.

- **High-Speed Serial Interface (HSSI):** Estándar de red para las conexiones seriales de alta velocidad (hasta 52 Mbps) sobre conexiones WAN.

3.1.4.2 Protocolos Capa Enlace de Datos WAN

describen cómo los marcos se llevan entre los sistemas en un único enlace de datos. Incluyen los protocolos diseñados para operar sobre recursos punto a punto dedicados, recursos multipunto basados en recursos dedicados, y los servicios conmutados multiacceso tales como Frame Relay.

- **Synchronous Data Link Control (SDLC).** Es un protocolo orientado a dígitos desarrollado por IBM. SDLC define un ambiente WAN multipunto que permite que varias estaciones se conecten a un recurso dedicado. SDLC define una estación primaria y una o más estaciones secundarias. La comunicación siempre es entre la estación primaria y una de sus estaciones secundarias. Las estaciones secundarias no pueden comunicarse entre sí directamente.

- **High-Level Data Link Control (HDLC)**. Es un estándar ISO. HDLC no pudo ser compatible entre diversos vendedores por la forma en que cada vendedor ha elegido cómo implementarla. HDLC soporta tantas configuraciones punto a punto como multipunto.

- **Link Access Procedure Balanced (LAPB)**. Utilizado sobre todo con X.25, puede también ser utilizado como transporte simple de enlace de datos. LAPB incluye capacidades para la detección de pérdida de secuencia o extravío de marcos, así como también para intercambio, retransmisión, y reconocimiento de marcos.

- **Frame Relay**. Utiliza los recursos digitales de alta calidad donde sea innecesario verificar los errores LAPB. Al utilizar un marco simplificado sin mecanismos de corrección de errores, Frame Relay puede enviar la información de la capa 2 muy rápidamente, comparado con otros protocolos WAN.

- **Point-to-Point Protocol (PPP)**. Descrito por el RFC 1661, dos estándares desarrollados por el IETF. El PPP contiene un campo de protocolo para identificar el protocolo de la capa de red.
- X.25. Define la conexión entre una terminal y una red de conmutación de paquetes.

- **Integrated Services Digital Network (ISDN).** Un conjunto de servicios digitales que transmite voz y datos sobre las líneas de teléfono existentes [32].

3.1.5 Elementos de Interconexión

independientemente de los protocolos utilizados, a diferencia con lo tradicional que era realizar la conexión a nivel de sistemas. Se conectaba cierto sistema de una red con su homólogo en la otra. Los equipos utilizados para la interconexión de redes WAN siguiendo el modelo de referencia OSI son:

Servidor: El servidor es aquel o aquellos ordenadores que van a compartir sus recursos hardware y software con los demás equipos de la red. Sus características son potencia de cálculo, importancia de la información que almacena y conexión con recursos que se desean compartir.
Repetidor: Se limita a la amplificación y regeneración de la señal a nivel físico. Las características más significativas son: permiten incrementar la longitud de red, operan con cualquier protocolo pues trabajan con señales físicas.

Puente (Bridge): Opera a nivel de enlace. Conecta redes homogéneas, es decir, que empleen igual protocolo de enlace. Es necesario para separar tráfico entre segmentos o para poder cumplir especificaciones de longitudes físicas o número de nodos conectados a dichos segmentos.

Encaminador (Router): Opera a nivel de red. Conecta redes de diferente topología (paso de testigo, ethernet, X.25). Permiten una distribución más efectiva del tráfico entre redes. Una aplicación adicional de los routers es actuar como pasarela de seguridad (firewall) entre la red propia y otra red. Este filtrado puede ser por dirección IP, por servicio (puerto) o a nivel de aplicación.

Pasarelas (Gateway): Son elementos de interconexión entre sistemas que realizan transformaciones a niveles superiores al nivel de red. Antes se utilizaban como elementos de interconexión, es decir, se salía de la red a través de un gateway para conectarse a otro sistema, limitando los servicios de conectividad a ese sistema, mientras que, en la actualidad, se tiende a conectar las redes mediante Routers y Bridges, con el gateway localizado en una de las redes como un servicio más. Un ejemplo de uso es transformar el correo X.400 en correo TCP/IP.

Switch: es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto.[17]

3.2 Clasificación de los Requerimientos Funcionales WAN

En la figura se muestra la clasificacion de los requerimientos funcionales de una red WAN, su clasificacion se divide de la siguiente manera:

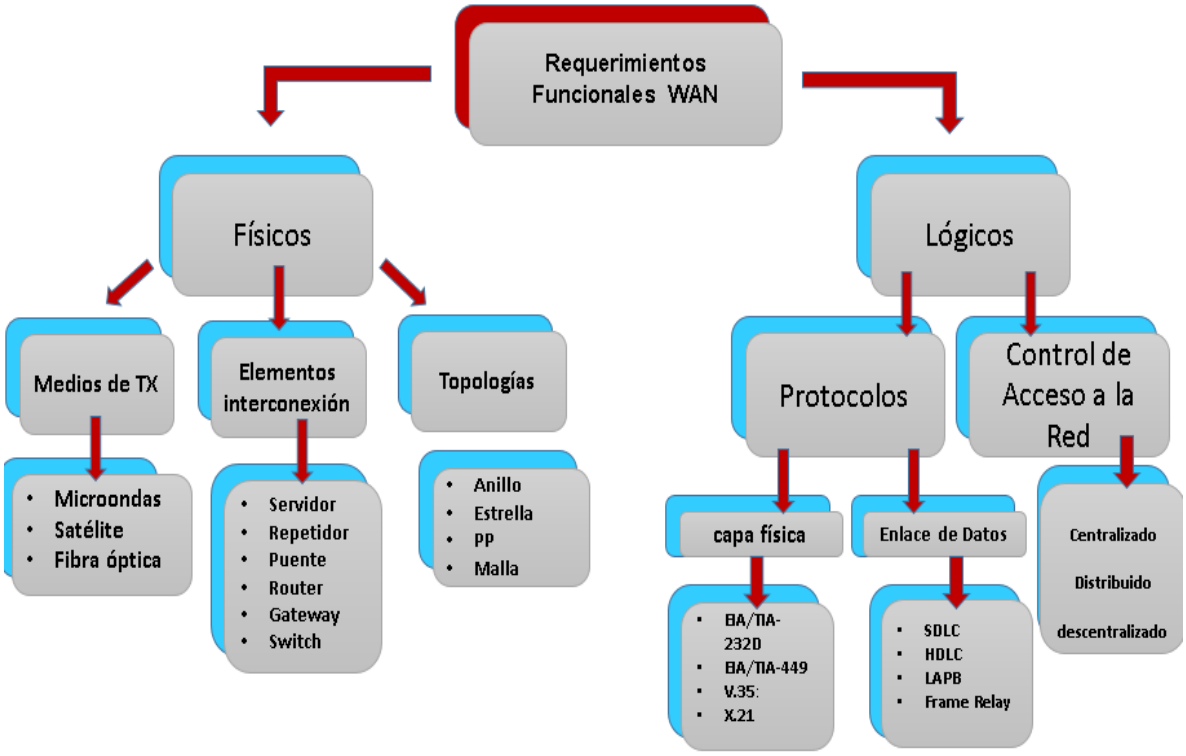


Figura 7. Clasificación Requerimientos Funcionales WAN

Capítulo 3

4. Procesos de desarrollo de Software

Un proceso se puede definir como una serie de operaciones o acciones que conducen a un fin. En general, una empresa u organización requiere de uno o más procesos para lograr sus objetivos, los cuales por lo general involucran la utilización de sistemas de software. En el caso de una empresa que se dedica al desarrollo de software, se requieren procesos que abarquen desde la creación de un sistema de software hasta su mantenimiento, Todo esto es conocido como el SDLC *(ciclo de vida desarrollo de software)*[33].

Para objeto del desarrollo de este trabajo se tendrán en cuenta las metodologías ISSAF (*Information System Security Assessment Framework)* y OSSTMM (*Open Source Security Testing Methodology Manual*) y a su vez el ciclo de vida de desarrollo de software en las que se enfocan de cada una de estas metodologías.

4.1 Fases ISSAF

La metodología de test de penetración ISSAF está diseñada para evaluar su Red de trabajo, sistema y control de aplicaciones. Está enfocada en tres fases y nueve pasos de evaluación. El enfoque incluye tres fases:

- Planificación y Preparación
- Evaluación
- Reportes, Limpieza y Destrucción de Objetos

4.1.1 Planificación y Preparación

En esta fase comprende los pasos iniciales para el intercambio de información, planificar y prepararse para la prueba. Antes de llevar a cabo la prueba formal de acuerdo será firmado por las ambas partes. Que constituye la base de esta tarea y la mutua protección jurídica. Asimismo, especificará la participación del equipo, las fechas exactas, los tiempos de la prueba, la escalada de privilegios y otros arreglos

Figura 8 . Fase 1 Y Sus Fases De Evaluacion**.**

4.1.2 Evaluación

Esta es la fase en donde lleva acabo el test de penetración. En la fase de evaluación en un enfoque por capas deberá ir seguida, como se muestra en la siguiente figura.

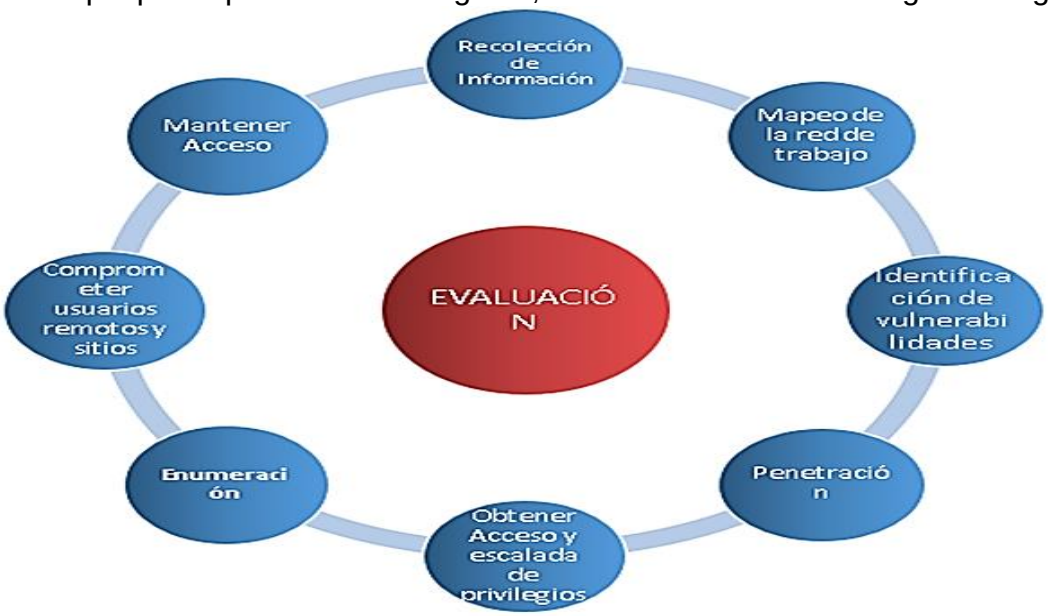


Figura 9. Fase 2 Y Sus Fases De Evaluacion**.**

Las fases de evaluacion se definen de la siguiente manera:

4.1.3 Reportes, Limpieza y Destrucción de Objetos

- **Informe Verbal:** Cuando realizan las pruebas de intrusión y posteriormente o durante esta se encuentra una amenaza, inmediatamente de debe informar a la organización.

- **Informe Final:** Cuando se finalizan las pruebas de intrusión se deben realizar un informe escrito y detallado que describa los resultados de la prueba.

- **Limpiar el sistema después de pruebas:** Remover todas las herramientas, archivos, software que se hayan instalado en el sistema [26].

4.2 Fases o Procesos OSSTMM

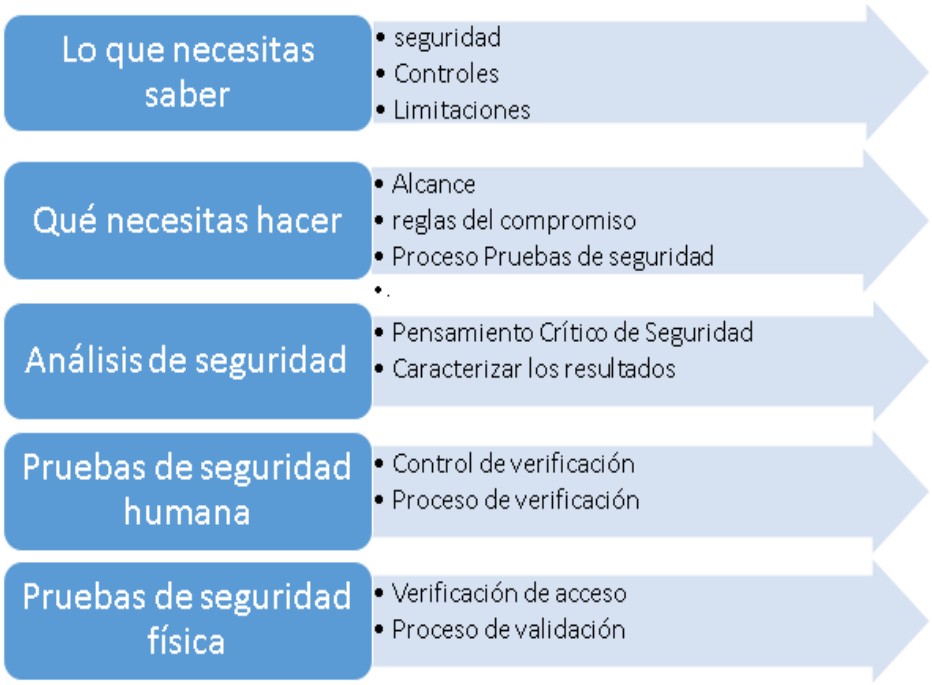


Figura 10. Fases OSSTMM**.**

4.2.1 Lo que Necesitas Saber

Esta metodología le dirá si lo que tienes hacer lo que quiere que haga y no sólo lo que le dijeron que hiciera. Para tener una verdadera seguridad de los bienes, se requieren diferentes tipos de controles. Sin embargo, los controles también pueden aumentar el número de interacciones dentro del alcance, lo que significa que más controles no son necesariamente mejor. Por lo tanto, se recomienda el uso de diferentes tipos de controles operacionales en lugar. Más controles del mismo tipo de controles operativos no proporcionan una defensa en profundidad como Acceso a través de uno es a menudo el acceso a través de todo ese tipo.

4.2.2 Que Necesitas Hacer

La sabiduría convencional dice que la complejidad es un enemigo de la seguridad. Sin embargo, sólo es en desacuerdo con la naturaleza humana. Cualquier cosa que se hace más compleja, no es inherentemente insegura. Considere la posibilidad de un ordenador la gestión de tareas complejas. El problema tal como la conocemos, no es que el equipo va a cometer errores, confundir las tareas, o se olvida de completar algunos. A medida que se agregan más tareas a la computadora, que se vuelve más lento y más lento, teniendo más tiempo para completar todas las tareas. La gente, sin embargo, cometen errores, se olvidan de tareas, abandonan las tareas que, o bien no son importantes o requerido en el momento. Así que cuando se prueba la seguridad, lo que hay que hacer es gestionar adecuadamente cualquier complejidad. Esto se hace definiendo adecuadamente la prueba de seguridad.

4.2.3 Análisis de Seguridad

Análisis de seguridad se refiere a la habilidad para convertir la información en inteligencia de seguridad. Esto requiere una comprensión más que sólo la información, sino también de dónde viene, cómo y cuándo se recogió y todas las restricciones del proceso de recolección. La parte final del proceso de análisis es la creación de inteligencia útil, la información derivada de hecho que puede ser utilizada para tomar decisiones. Esta es la clara distinción entre la seguridad y análisis de riesgo. En el análisis de seguridad, se produce incluso si los hechos que los estados de hecho algo que no puede ser conocido a partir de la información proporcionada. En el análisis de riesgos, especular y obtener opiniones basadas en la información.

4.2.4 Pruebas de Seguridad Humana

Seguridad Humana (HUMSEC) es una subsección de la física e incluye las operaciones psicológicas (PSYOPS). este canal requiere la interacción con las personas en posiciones de gatekeeper de activos.
Este canal cubre la participación de las personas, sobre todo el personal que opera dentro del ámbito o el marco de destino. Mientras que algunos servicios consideran este simplemente como "ingeniería social", el verdadero objetivo de las pruebas de cumplimiento de la seguridad en este canal es la prueba de concienciación sobre la seguridad personal y la medición de la brecha con el estándar de seguridad requerido se indica en la política de la empresa, regulaciones de la industria, o la legislación regional.

4.2.5 Pruebas de Seguridad Fisica

Es una clasificación para la seguridad material dentro del reino físico que está dentro de los límites del espacio humano 3D interactivo. Prueba de este canal requiere la interacción no comunicativa con las barreras y los seres humanos en posiciones de gatekeeper de activos.
Este canal cubre la interacción del analista dentro de la proximidad de los blancos. Mientras que algunos servicios consideran que esto simplemente como "allanamiento de morada", el verdadero objetivo del cumplimiento de las pruebas de seguridad en este canal es la prueba de barrera física y lógica y la medición de la brecha con el estándar de seguridad requerido como se indica en la política de la empresa, regulaciones de la industria, o la legislación regional [34]

4.3 SDLC OWASP

Durante el ciclo de vida del desarrollo de una aplicación web, muchas cosas han de ser probadas

- Poner a prueba o probar
- Pasar una prueba
- Ser asignado un estado o evaluación basado en prueba

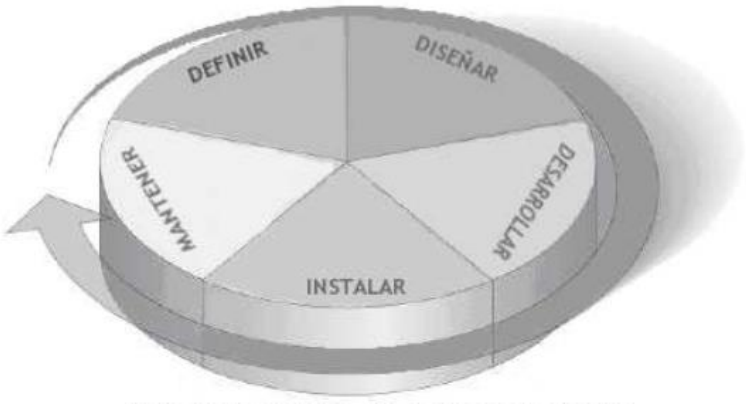


Figura 11. Modelo SDLC Genérico [35]

4.3.1 Antes de Empezar el Desarrollo

Antes de que el desarrollo de la aplicación haya empezado:

- Comprobación para asegurar que existe un SDLC adecuado, en el cual la seguridad
- sea inherente. Comprobación para asegurar que están implementados la política y estándares de seguridad adecuados para el equipo de desarrollo.
- Desarrollar las métricas y criterios de medición.

4.3.1.1 Fase 1A: Revisión de Estándares y Políticas

Asegurar que las políticas, documentación y estándares adecuados están implementados. La documentación es extremadamente importante, ya que brinda al equipo de desarrollo políticas y directrices a seguir.

4.3.1.2 FASE 1B: Desarrollo de Métricas y Criterios de Medición

Antes de empezar el desarrollo, planifica el programa de medición. Definir los criterios que deben ser medidos proporciona visibilidad de los defectos tanto en el proceso como en el producto. Es algo esencial definir las métricas antes de empezar el desarrollo, ya que puede haber necesidad de modificar el proceso (de desarrollo) para poder capturar los datos necesarios

4.3.2 Durante el Diseño y Definición

4.3.2.1 Fase 2A: Revisión de los Requisitos de Seguridad

Los requisitos de seguridad definen como funciona una aplicación desde una perspectiva de la seguridad. Es indispensable que los requisitos de seguridad sean probados. Probar, en este caso, significa comprobar los supuestos realizados en los requisitos, y comprobar si hay deficiencias en las definiciones de los requisitos.

Por ejemplo, si hay un requisito de seguridad que indica que los usuarios deben estar registrados antes de tener acceso a la sección de Documentos de un sitio, ¿Significa que el usuario debe estar registrado con el sistema, o debe estar autenticado? Asegúrate de que los requisitos sea lo menos ambiguo posible.

A la hora de buscar inconsistencias en los requisitos, ten en cuenta mecanismos de seguridad como:

- Gestión de Usuarios (reinicio de contraseñas, etc.)
- Autenticación
- Autorización
- Confidencialidad de los Datos
- Integridad
- Contabilidad
- Gestión de Sesiones
- Seguridad de Transporte
- Segregación de Sistemas en Niveles
- Privacidad

4.3.2.2 Fase 2B: Revisión de Diseño y Arquitectura

Las aplicaciones deberían tener una arquitectura y diseño documentados. Por documentados nos referimos a modelos, documentos de texto y semejantes. Es indispensable comprobar estos elementos para asegurar que el diseño y la arquitectura imponen un nivel de seguridad adecuado al definido en los requisitos.

4.3.2.3 Fase 2C: Creación y Revisión De Modelos UML

Una vez completados el diseño y arquitectura, construye modelos de Lenguaje Unificado de Modelado (de ahora en adelante y por sus siglas en inglés, Unified Modeling Language, UML), que describan cómo funciona la aplicación. En algunos casos, pueden estar ya disponibles. Emplea estos modelos para confirmar junto a los diseñadores de sistemas una comprensión exacta de cómo funciona la aplicación. Si se descubre alguna vulnerabilidad, debería serle transmitida al arquitecto del sistema para buscar soluciones alternativas.

4.3.2.4 Fase 2D: Creación y Revisión de Modelos de Amenaza

Con las revisiones de diseño y arquitectura en mano, y con los modelos UML explicando cómo funciona el sistema exactamente, es hora de acometer un ejercicio de modelado de amenazas. Desarrolla escenarios de amenaza realistas. Analiza el diseño y la arquitectura para asegurarte de que esas amenazas son mitigadas, aceptadas por negocio, o asignadas a terceros, como puede ser una aseguradora. Cuando las amenazas identificadas no tienen estrategias de mitigación, revisa el diseño y la arquitectura con los arquitectos de los sistemas para modificar el diseño.

4.3.3 Durante El Desarrollo

En teoría, el desarrollo es la implementación de un diseño. Sin embargo, en el mundo real, muchas decisiones de diseño son tomadas durante el desarrollo del código. A menudo son decisiones menores, que o bien eran demasiado detalladas para ser descritas en el diseño o, en otras cosas, incidencias para las cuales no había ninguna directriz o guía que las cubriese. Si la arquitectura y el diseño no eran los adecuados, el desarrollador tendrá que afrontar muchas decisiones. Si las políticas y estándares eran insuficientes, tendrá que afrontar todavía más decisiones.

4.3.3.1 Fase 3A: Inspección de Código por Fases

El equipo de seguridad debería realizar una inspección del código por fases con los desarrolladores y, en algunos casos, con los arquitectos del sistema. Una inspección de código por fases es una inspección del código a alto nivel, en la que los desarrolladores pueden explicar el flujo y lógica del código. Permite al equipo de revisión de código obtener una comprensión general del código fuente, y permite a los desarrolladores explicar porque se han desarrollado ciertos elementos de un modo en particular.

4.3.3.2 Fase 3b: Revisiones de Código

Con una buena comprensión de cómo está estructurado el código y porque ciertas cosas han sido programadas como lo han sido, el probador puede examinar ahora el código real en busca de defectos de seguridad.

4.3.4 Durante la Implementación

4.3.4.1 Fase 4A: Pruebas de Intrusión en Aplicaciones

Tras haber comprobado los requisitos, analizado el diseño y realizado la revisión de código, debería asumirse que se han identificado todas las incidencias. Con suerte, ese será el caso, pero las pruebas de intrusión en la aplicación después de que haya sido. implementada nos proporciona una última comprobación para asegurarnos de que no se nos ha olvidado nada.

4.3.4.2 Fase 4B: Comprobación de Gestión De Configuraciones

La prueba de intrusión de la aplicación debería incluir la comprobación de cómo se implementó su infraestructura. Aunque la aplicación puede ser segura, un pequeño detalle de la configuración podría estar en una etapa de instalación predeterminada, y ser vulnerable a explotación.

4.3.5 Mantenimiento y Operaciones

4.3.5.1 Fase 5A: Ejecución de Revisiones de la Administración Operativa

Debe existir un proceso que detalle cómo es gestionada la sección operativa de la aplicación y su infraestructura.

4.3.5.2 Fase 5B: Ejecución de Comprobaciones Periódicas de Mantenimiento

Deberían realizarse comprobaciones de mantenimiento mensuales o trimestrales, sobre la aplicación e infraestructura, para
asegurar que no se han introducido nuevos riesgos de seguridad y que el nivel de seguridad sigue intacto.

4.3.5.3 Fase 5c: Asegurar La Verificación De Cambios

Después de que cada cambio haya sido aprobado, testeado en el entorno de QA e implementado en el entorno de producción, es vital que, como parte del proceso de gestión de cambios, el cambio sea comprobado para asegurar que el nivel de seguridad no haya sido afectado por dicho cambio [35].

Capítulo 4

5. Pruebas con Owasp-Zap y Openvas de kali Linux 2.0

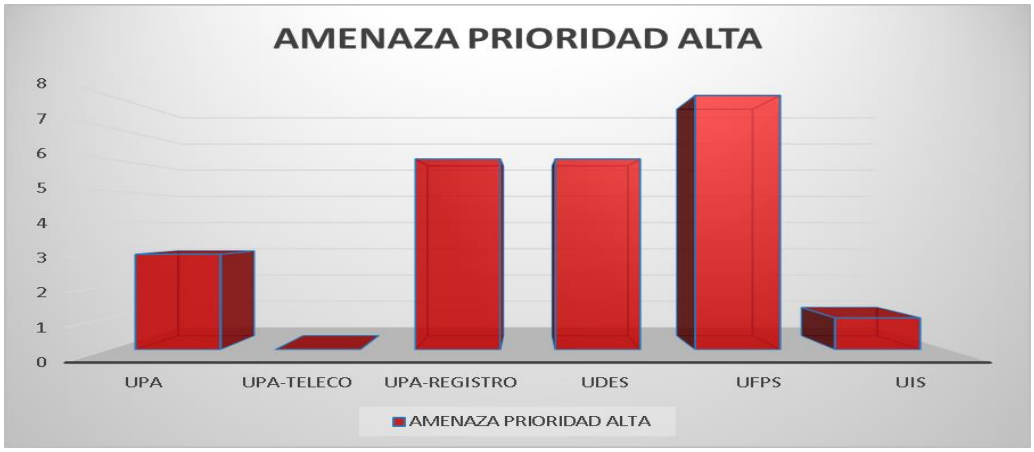
5.1 Pruebas Con Owasp- Zap

A continuación, se mostrarán y se podrá observar las estadísticas de las pruebas y análisis de vulnerabilidad realizados a las aplicaciones web de algunas de las universidades de la región como lo son UPA, UFPS, UIS, UDES, con la ayuda del sistema operativo KALI LINUX 2.0 y a su vez el software OWASP-ZAP

.

En la gráfica se muestra el resultado del análisis realizado con la ayuda de OWAS-ZAP y cuya interpretación demuestra que la aplicación web de la UFPS, es la de mayor vulnerabilidad y la de Telecomunicaciones de la UPA es la menor, todo este análisis técnico lo podemos lo detallamos mejor en los anexos.

ver en **Anexo A**

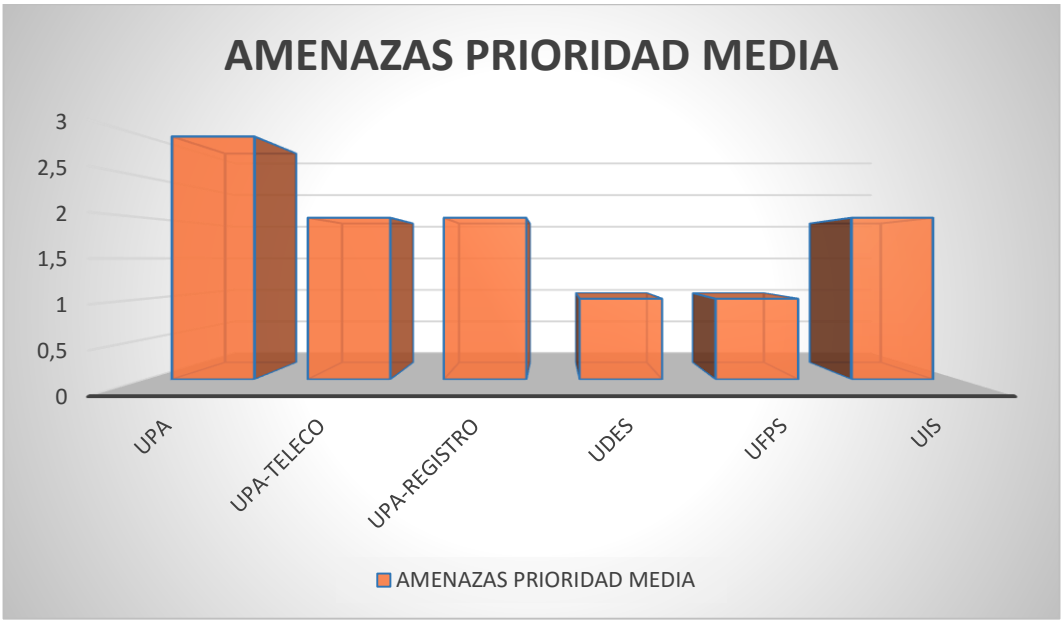


Grafica 2. Amenazas prioridad Alta

NUMERO DE AMENAZAS ALTAS	
UPA	**3**
UPA-TELECO	**0**
UPA-REGISTRO	**6**
UDES	**6**
UFPS	**8**
UIS	**1**

Tabla 1. Numero de amenazas a aplicaciones escaneadas con prioridad alta.

En la gráfica se muestra el resultado del análisis realizado con la ayuda de OWAS-ZAP y cuya interpretación demuestra que la aplicación web de la UPA, es la de mayor riesgo a niveles de amenazas de prioridad media. Todo este análisis técnico lo podemos lo detallamos mejor en anexos.
ver en **Anexo A**.

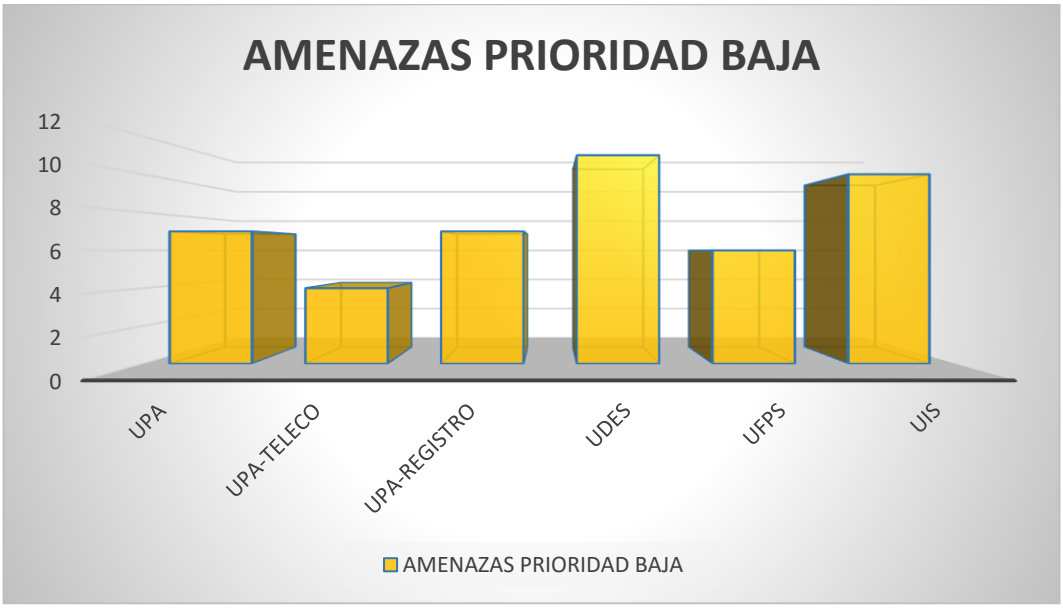


Grafica 3. Amenazas Nivel Medio.

NUMERO DE AMENAZAS NIVEL MEDIO	
UPA	3
UPA-TELECO	2
UPA-REGISTRO	2
UDES	1
UFPS	1
UIS	2

Tabla 2. Numero de amenazas a aplicaciones escaneadas con prioridad media

En la gráfica se muestra el resultado del análisis realizado con la ayuda de OWAS-ZAP y cuya interpretación demuestra que la aplicación web de UDES, es la de mayor riesgo a niveles de amenazas de prioridad baja.
todo este análisis técnico lo podemos lo detallamos mejor en nuestros anexos.
ver en **Anexo A**



Grafica 4. Amenazas Nivel Bajo.

NUMERO DE AMENAZAS NIVEL BAJO	
UPA	3
UPA-TELECO	2
UPA-REGISTRO	2
UDES	1
UFPS	1
UIS	5

Tabla 3. Numero de amenazas a aplicaciones escaneadas con prioridad BAJA

En la gráfica se muestra el resultado del análisis realizado con la ayuda de OWAS-ZAP y cuya interpretación demuestra que la aplicación web de UDES, es la de mayor riesgo a niveles de alertas de tipo informativas. Todo este análisis técnico lo podemos lo detallamos mejor en nuestros anexos.
ver en **Anexo A**.

Grafica 5. Amenazas Nivel Informativo.

NUMERO DE AMENAZAS NIVEL BAJO	
UPA	3
UPA-TELECO	2
UPA-REGISTRO	2
UDES	1
UFPS	1
UIS	5

Tabla 4. Numero de amenazas a aplicaciones escaneadas de nivel informativo.

5.2 Pruebas con Openvas

Con la ayuda de comandos en el Terminal de Kali Linux se puede determinar los puertos abiertos de una aplicación web, todo esto con el fin de que al momento de configurar OPENVAS solo se realice el escaneo y análisis de únicamente estos puertos, para no gastar recursos ni tiempo.

A continuación, se observarán un conjunto de figuras que demuestran los procedimientos que se llevan a cabo para obtener que puertos están abiertos y con qué protocolo trabajan.

En la siguiente figura, se observa que los puertos 53 y 8000, utilizando el protocolo TCP se encuentran abiertos para la aplicación web de la universidad de pamplona.

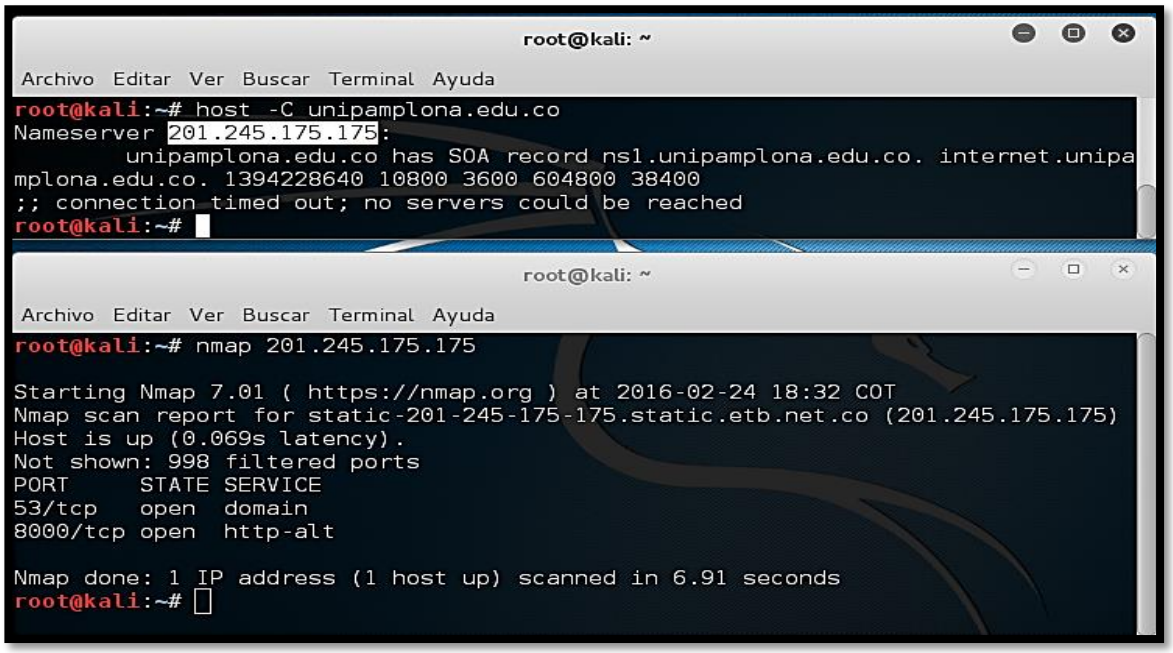


Figura 12. Análisis de puertos para UPA

En la siguiente figura, se observa que es no es posible observar que puertos se encuentran abiertos para la aplicación web de la UDES, debido a que cuenta con un tipo de restricción de seguridad implementado tal vez por un firewall o un bloqueo en los servidores, impidiendo las pruebas de ping que realizan para observar tales puertos.

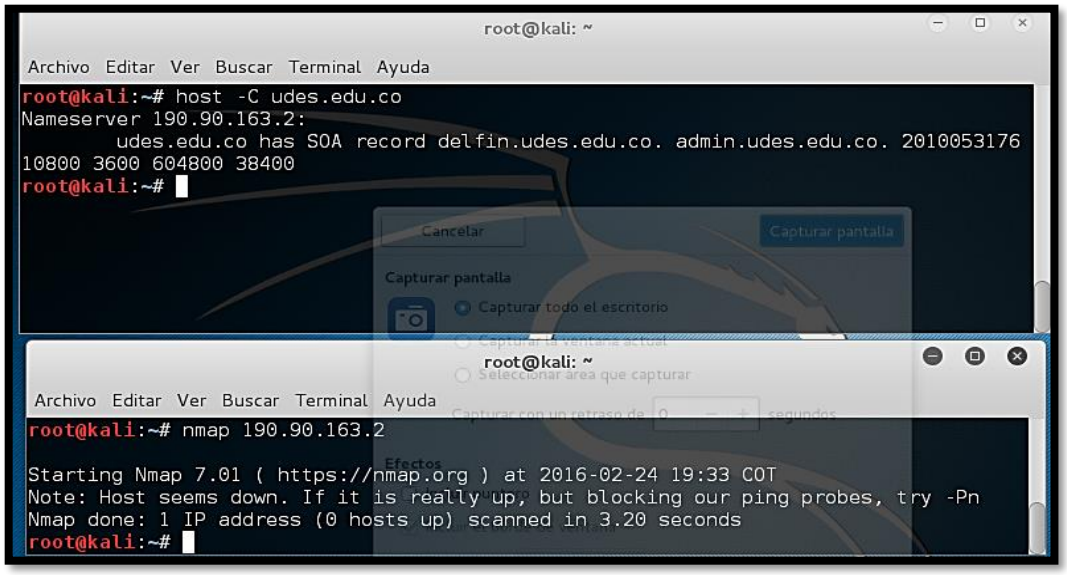


Figura 13. Análisis de puertos para UDES.

En la siguiente figura, se observa que es no es posible observar que puertos se encuentran abiertos para la aplicación web de la UIS, debido a que cuenta con un tipo de restricción de seguridad implementado tal vez por un firewall o un bloqueo en los servidores, impidiendo las pruebas de ping que realizan para observar tales puertos.

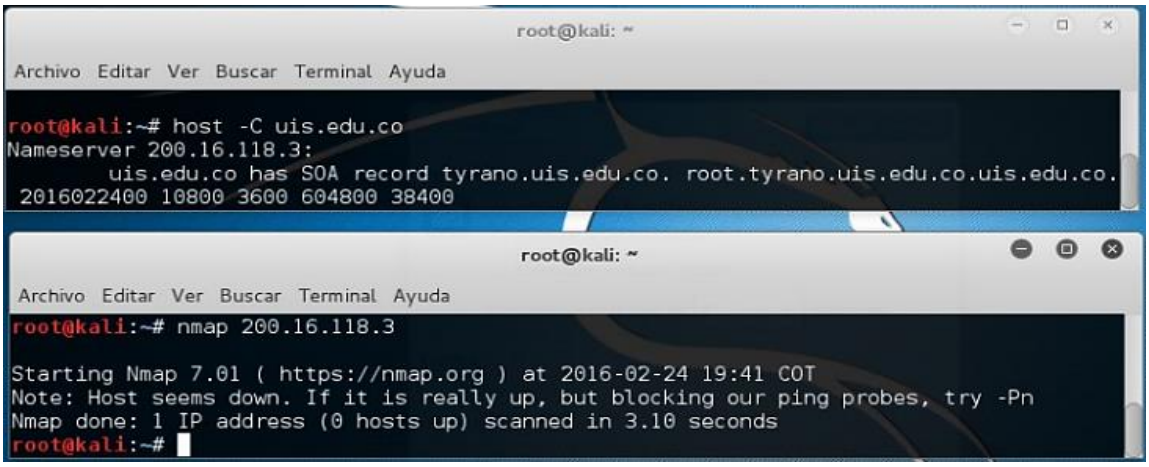


Figura 14. Análisis de puertos para UDES

En la siguiente figura, se observa que los puertos 20, 21, 25, 53, 80, 110, 143, 443, utilizando el protocolo TCP se encuentran abiertos para la aplicación web de la UFPS.

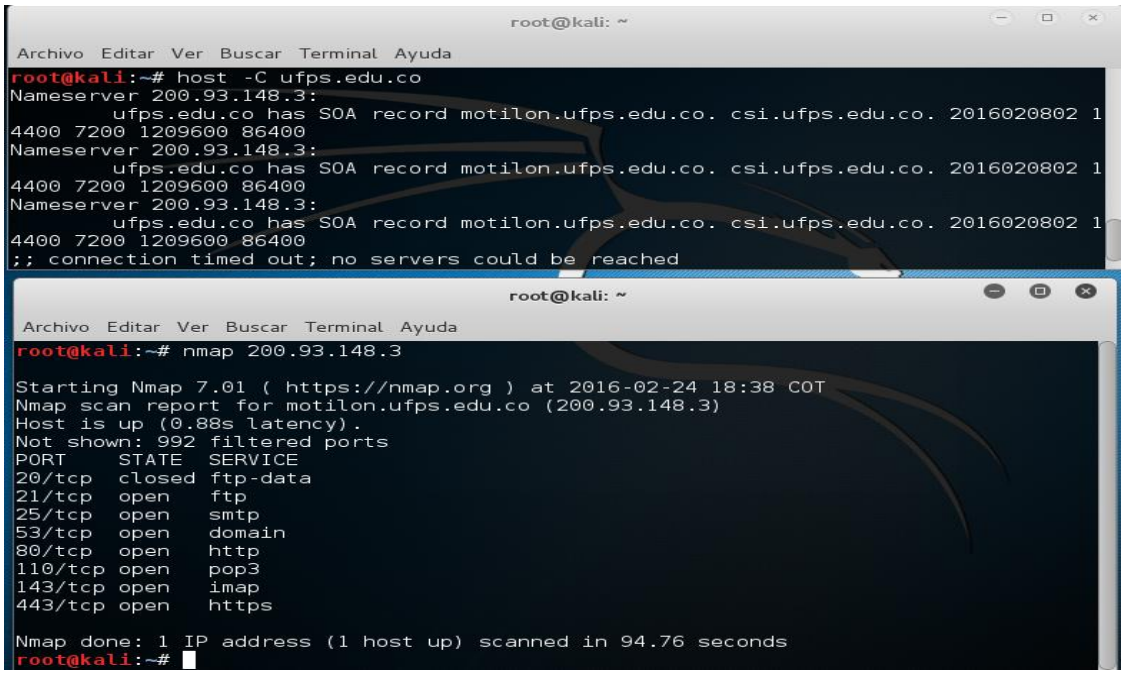


Figura 15. Análisis de puertos para UFPS.

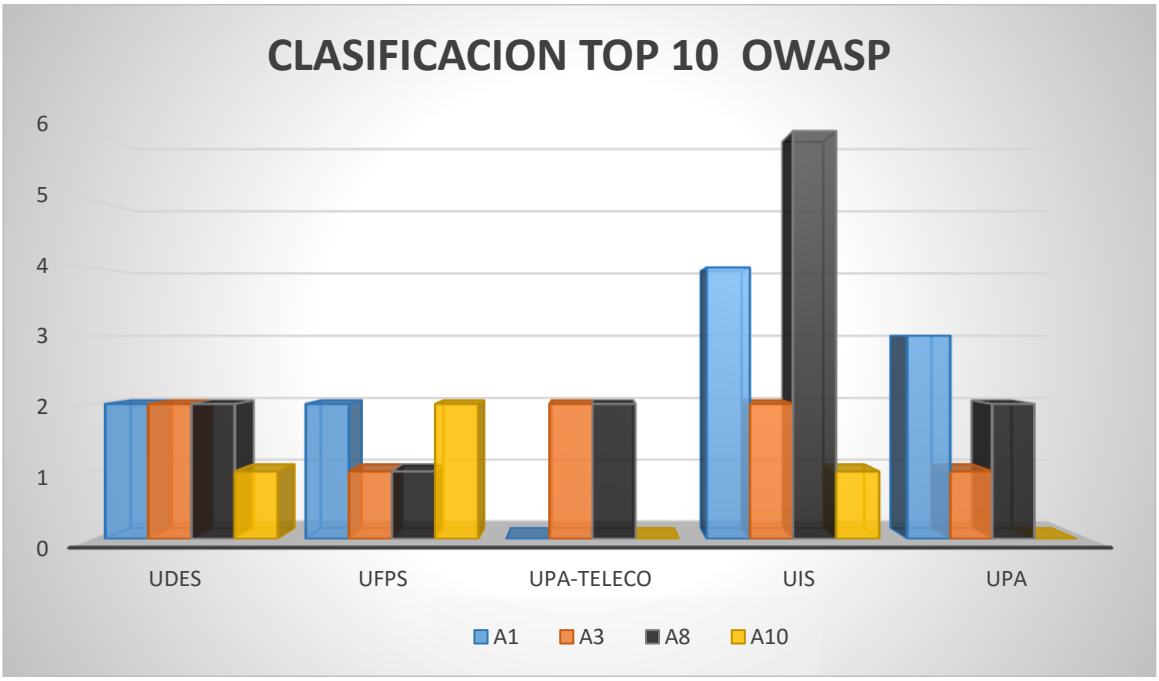
En la tabla 5, se muestra el resultado del escaneo de vulnerabilidades realizados con la ayuda de la herramienta de software OPENVAS, cuyo resultado arroja que en la universidad de pamplona para un escaneo tipo FULL AND FAST y con una selección de puertos mostrados en la Figura 8 la exposición o el nivel de riesgo es bajo con 1 amenaza, y para la universidad Francisco de Paula Santander no se encontró ningún tipo de exposición para el escaneo de puertos definidos en la Figura 12. **Ver Anexo B**

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Wed Feb 4 22:52:35 2016	Done	UFPS TAREA	0.0 (Log)	0	0	0	21	0	
Wed Feb 4 00:04:52 2016	Done	unipamplona	2.6 (Low)	0	0	1	17	0	
							√Apply to page contents		
(Applied filter: apply_overrides=1 rows=10 sort-reverse=date first=1)							1 - 2 of 2 (total: 2)		

Tabla 5. Numero de Vulnerabilidades con OPENVAS para UPA y UFPS

5.3 Clasificación de Vulnerabilidades Top 10 Owasp

Teniendo en cuenta los resultados arrojados por el análisis de vulnerabilidad realizado con la ayuda del sistema operativo KALI LINUX Y el software OWASP-ZAP la clasificación dentro del top 10 de la metodología OWASP para las vulnerabilidades encontradas dentro del informe técnico (ver **anexo A**), tenemos:



Grafica 6. Clasificación vulnerabilidades TOP 10 OWASP**.**

A1- Inyección: Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder datos no autorizados.

A3 – Secuencia de Comandos en Sitos Cruzados (XSS): Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.

A8 - Falsificación de Peticiones en Sitos Cruzados (CSRF): Un ataque CSRF obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la víctima para generar pedidos que la aplicación vulnerable piensa son peticiones legítimas provenientes de la víctima.

A10 – Redirecciones y Reenvíos no Validados: Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder páginas no autorizadas [36].

5.4 Propuesta de Clasificación de los Procesos de Desarrollo de Software

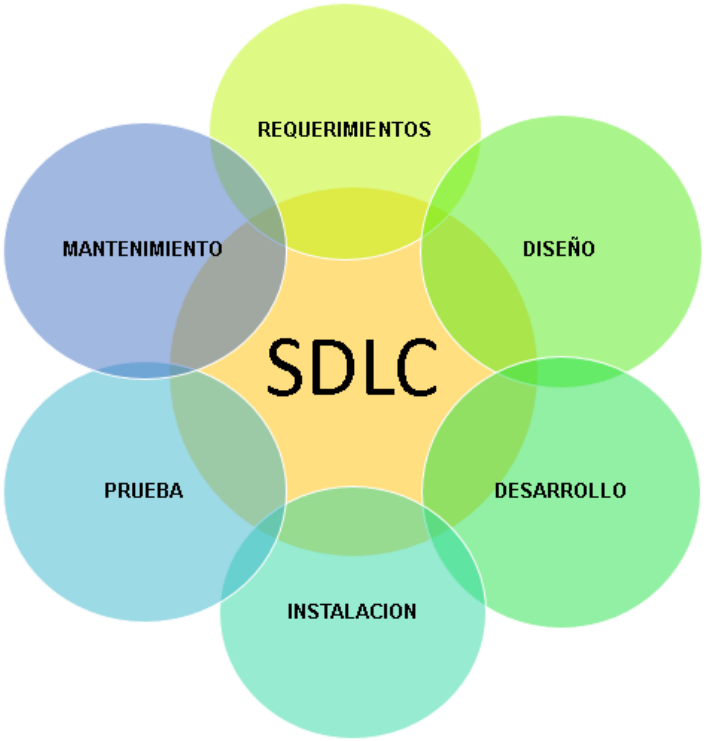


Figura 16. Propuesta SDLC

5.4.1 Fase 1: Análisis de Requerimientos

análisis de requerimientos es la primera etapa, es la más importante de cualquier modelo SDLC. Esta fase es básicamente la fase de intercambio de ideas, ya que tiene las muchas etapas para sub etapas de análisis de viabilidad como para comprobar cuántas ideas se pueden poner en acción para el desarrollo.

5.4.2 Fase 2: Diseño

En esta fase, el diseño ha sido desarrollado por los analistas y diseñadores. El analista de sistemas crea el diseño lógico para los diseñadores y luego el diseñador consigue la idea básica de esbozar el diseño de software
El diseñador y Analista de sistemas trabajan juntos en el diseño del software, permitiendo así una mejor integración de conocimientos en pro del desarrollo del software.

5.4.3 Fase 3: Desarrollo

En esta etapa, Se ejecutan las ideas de los analistas, programadores y diseñadores se desarrollan todos los borradores propuestos y avalados por la “junta”, su objetivo principal es determinar y exponer un prototipo del producto que va a ser lanzado al mercado, pero esta no será la última etapa de este ciclo, posteriormente se implementa o instala.

5.4.4 Fase 4: Instalación

Luego de que se haya comprobado de que el software no sufre ningún tipo de defecto, se aplican todas las herramientas que le permitan colocar en funcionamiento el software, pero aún no está listo para ser lanzado al mercado o facilitárselo al comprador.

5.4.5 Fase 5: Prueba

Errar es humano y la etapa de pruebas tiene como objetivo detectar los errores que se hayan podido cometer en las etapas anteriores del proyecto (y, eventualmente, corregirlos). Lo suyo, además, es hacerlo antes de que el usuario final del sistema los tenga que sufrir. De hecho, una prueba es un éxito cuando se detecta un error (y no al revés, como nos gustaría pensar).

5.4.5 Fase 6. Mantenimiento

En esta etapa, luego de verificar que no existe ningún error en los procesos de desarrollo del software, se lanza al mercado, y constantemente se le da un soporte al usuario para siga utilizando el software y para enseñarlo, instruirlo y ayudarlo en caso de que este tenga algún tipo de modificación o actualización.

Capítulo 5

6. Herramientas de Software Licenciados y no Licenciados

Vivimos en una era tecnológica en la que cada aspecto de nuestra vida está ligado, directa o indirectamente, a ella. La información está en la palma de nuestras manos, nada es restringido, nada es desconocido, y aquello que parecía imposible hace más de una década, hoy lo podemos hacer con un solo “clic”.
Gracias a la internet y a los adelantos que esta conlleva, la forma que nos relacionamos, estudiamos, vivimos, comercializamos e interactuamos ha cambiado radicalmente. Actualmente y desde hace muchos años algunos teníamos la posibilidad de interactuar, utilizar software libre/ software propietario, pero no hemos tenido un concepto claro de lo que significa cada uno de estos tipos de software.[37]

6.1 Software no Licenciado

Es importante tener en cuenta que al hablar de software libre no siempre significa gratuito, significa dominio sobre el código de construcción, cosa que no permite en absoluto el software licenciado. Entonces se pueden encontrar desarrollos de aplicativos hechos en software libre que son distribuidos comercialmente y con un costo de adquisición, teniendo el nuevo propietario capacidad de modificar su funcionamiento al tener conocimiento de la programación de este. Bajo esta aclaración inicial y de acuerdo al costo o no de distribución encontramos una gama de tipologías de software como son: Software de código fuente abierto, Software de dominio público, Software con copyleft, Software semilibre, Software propietario, Freeware, Shareware, Software comercial, todos ellos con caracterizaciones especificas en su distribución, licenciatura y costo.

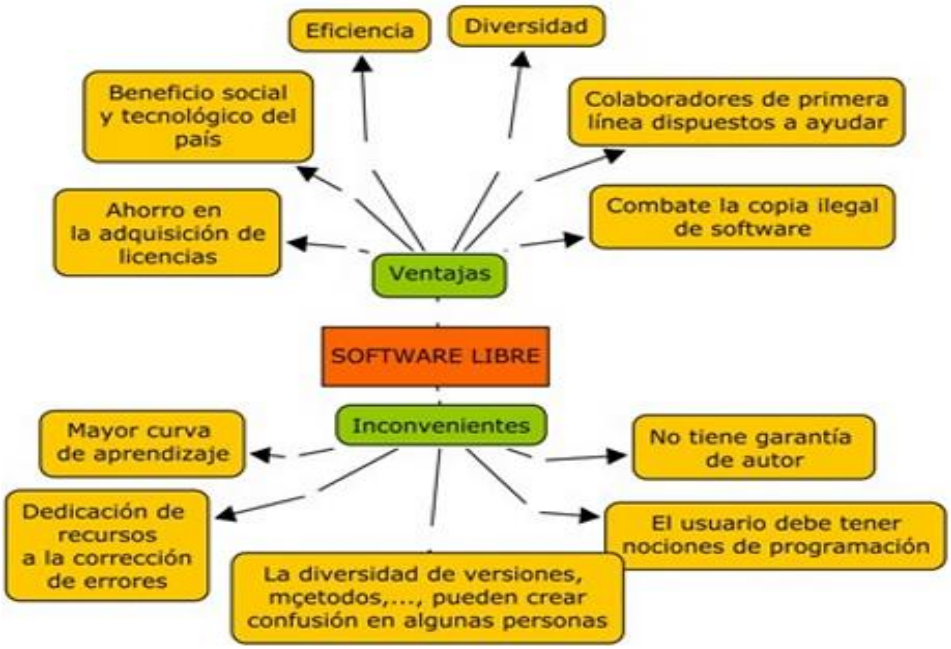


Figura 17. Ventajas y desventajas software libre [38]

6.1.1 Ejemplos de Software no Licenciados

Ettercap: Ettercap es una utilidad que nos permite capturar el tráfico que circula por una WAN, ya sea en un ambiente switcheado (lo crean o no) o HUBeado. O sea, es un sniffer. Nos provee de dos modos de funcionamiento: INTERACTIVO y NO-Interactivo. Todo se controla por letras-comando, más los cursores y el enter, y en cada pantalla del modo interactivo pueden tilizar el comando 'h', para obtener un breve listado de comandos en el area actual del programa. Para salir o volver atras, pueden utilizar 'q'.

Driftnet: captura el tráfico de imágenes en una red y los muestra en una carpeta predeterminada, observa tráfico de red y escoge y muestra imágenes JPEG y GIF para la exhibición. Es una invasión de la privacidad horrible y no debe ser utilizado por cualquier persona en cualquier lugar [39] .

6.2 Software Licenciado

El software licenciado básicamente es aquel que oculta completamente el código de construcción (programación ejecutable), otorgando así en un intercambio comercial el permiso de funcionamiento, alquiler u utilización establecidos por el constructor o fabricante, generalmente grandes empresas que son potencia en desarrollo de software [38].
posee restricciones en el uso, copia o modificación (código cerrado). Que un software haya liberado su código no implica necesariamente que sea un software libre sino que también puede ser propietario [40].

Figura 18. Ventajas y desventajas software licenciados [38]

6.2.1 Ejemplos de Software Licenciados que Permiten la Detección de Amenazas

Fortinet: proporciona actualizaciones totalmente automatizada para asegurar la protección contra las últimas amenazas a nivel de contenido. Emplea avanzada de virus, software espía, y los motores de detección heurística para proteger FortiGate, FortiMail, aparatos FortiWiFi, y los agentes de seguridad de punto final FortiClient, evitar a las nuevas y cambiantes amenazas puedan acceder a contenidos de valor y las aplicaciones de la red. Fortinet proporciona actualizaciones globales a través de la Red de Distribución de FortiGuard para una protección completa contra todas las amenazas a nivel de contenido [41].

Panda: antivirus un producto anti-malware era una de las mejores marcas de software para proteger el pc. Hoy en dia software como por ejemplo SpyHunter son evaluados con una mejor nota .
Este producto ofrece la seguridad completa para las amenazas en internet. Panda software es un producto español y fundado en 1990 en Bilbao, donde en corto tiempo se convirtió en uno de los antivirus más avanzados en el mundo. Recientemente Panda antivirus ha cambiado su nombre a PANDA SECURITY. [42].

Avira: protege sus datos y su privacidad y bloquea todos los tipos de software malicioso, incluidos virus, gusanos, troyanos y spyware [43].

Bitdefender: presenta una arquitectura escalable y basada en distintos motores para diferentes tipos de archivos y malware, que se cargan en tiempo real, sin necesidad de reconfigurar o reiniciar el sistema [44].

Kaspersky: ofrece protección esencial contra todos los tipos de software malicioso. Es el ingrediente clave para defender tu equipo y resguardarte de los últimos virus, spyware, gusanos y más. Es una solución de seguridad fácil de usar que no afectará tu rendimiento.[45]

Nod32: Es un programa antivirus desarrollado por la empresa ESET, de origen eslovaco. El producto está disponible para Windows, Linux, FreeBSD, Solaris, Novell y Mac OS X (este último en beta), y tiene versiones para estaciones de trabajo, dispositivos móviles (Windows Mobile y Symbian, servidores de archivos, servidores de correo electrónico, servidores gateway y una consola de administración remota [46].

Mcafee: reconoce las amenazas de Internet de la actualidad, McAfee Total Protection protege su PC, red social, identidad, familia y su red doméstica con nuestra última protección frente a piratas informáticos, malware, spyware, phishing y otras amenazas online [47].

6.3 Algoritmos que Permiten la Detección de Amenazas

Actualmente no existen algoritmos que permitan la detección de vulnerabilidades o amenazas, lo que conocemos hoy en día como antivirus utilizan una base de datos actualizable de malware que incorporan y que solo permite la identificación mediante la comparación al momento de realizar el análisis con la amenaza detectada y la base de datos, cabe decir que todo esto se ha venido comportando de esta manera durante todo este tiempo por fines comerciales ya que las empresas que se dedican a crear este tipo de software no les interesa crear un algoritmo que permita detectar y eliminar un malware, por qué el usuario al adquirir una nueva versión de este software les representaría constantemente unos ingresos económicos gigantescos, pero esto tiende a cambiar tal y como lo expone el doctor *Kevin Hamlen* de la Universidad de Texas en Dallas .

actualmente la mayoría de los virus se propagan al azar a través de la Red, mutando para evitar ser copias exactas y dificultar así su detección.

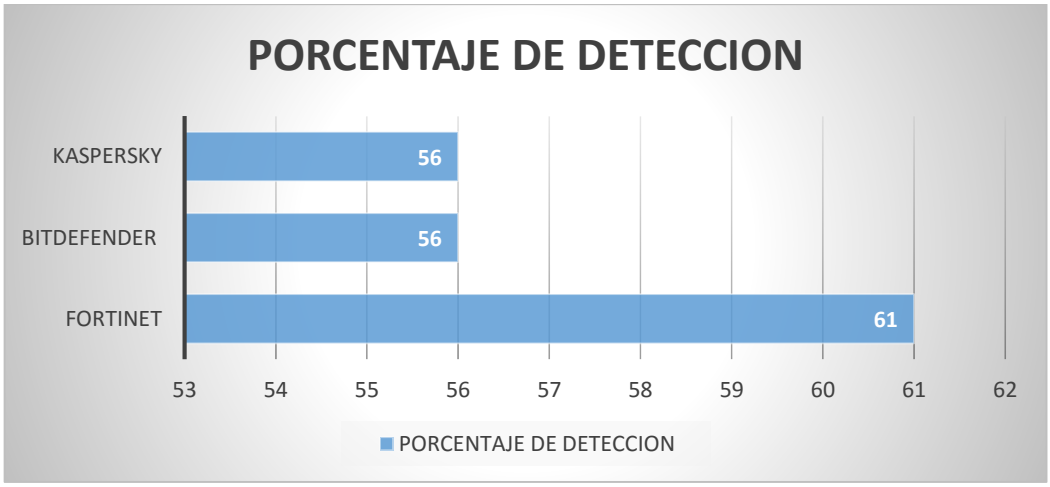
“Lo que nuestra investigación estaba viendo era si estos virus podrían empeorar al mutar de forma directa en lugar de al azar, de modo que pudieran infectar una máquina, detectar qué tipo de defensas tiene, aprender sobre ellas utilizando avanzadas técnicas automáticas, y luego trabajar activamente para derrotarlas a través de la Red”, detalló el informático.

Por eso su proyecto, más que perfeccionar los actuales sistemas de detección de malware, pretende anticiparse a la acción de esos códigos malignos. Para ello, Hamlen plantea aplicar los avances en el lenguaje de programación a la investigación de software de seguridad. Como se menciona también en un comunicado la propia Universidad de Texas, la idea es “implementar algoritmos que capten el código sospechoso cuando va a empezar a ejecutarse, e interrumpirlo en los microsegundos entre las pruebas de daño inminente y el daño real en sí”, extrapolando la fórmula que usan los programadores informáticos para tratar de predecir lo que los programas hacen una vez que los ejecutan[48]

6.4 Clasificación de Herramientas que Permiten la Detección de Amenazas

Buenos

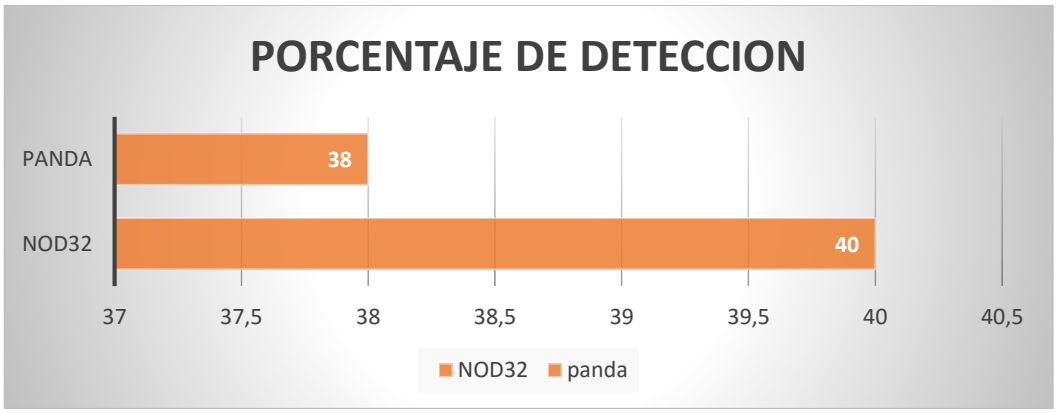
Permiten un número considerable de detección de amenazas.



Grafica 7. Porcentaje de detección bueno.

Regulares

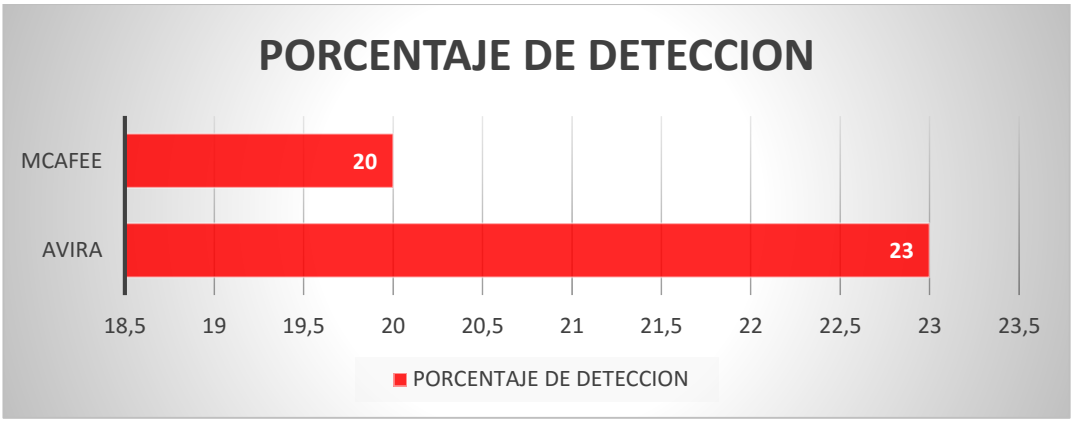
Permite un numero aceptable de detección de amenazas



Grafica 8 Porcentaje de detección regular

Malos

Permite un número mínimo de detección de amenazas



Grafica 9. Porcentaje de detección MALAS

El reporte anteriormente mencionado y la clasificación realizada, se basan en el reporte generado por las pruebas independientes de software antivirus [49]

Capítulo 6

7. Escenarios y Agujeros de Seguridad en una Red WAN

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar vulnerabilidades en el diseño, configuración y operación de los sistemas, esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres, que en muchos casos llevaron a la desaparición de aquellas organizaciones (en su mayoría fueron empresas que poseían altísimo grado de dependencia tecnológica, como bancos, servicios automáticos, etc). Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita un conocimiento técnico básico para realizarlos. Se han clasificado las generaciones de ataques en la red existentes a lo largo del tiempo para una red WAN, como se muestra a continuación:

La primera generación: Ataque Físico: Ataques que se centraban en los componentes electrónicos como ordenadores, dispositivos y cables.

La segunda generación: Ataque Sintáctico Las pasadas décadas se han caracterizado por ataques contra la lógica operativa de los ordenadores y las redes, es decir, pretendían explotar las vulnerabilidades

La tercera generación: Ataque Semántico Se basan en la manera en que los humanos asocian significado a un contenido. El inicio de este tipo de ataques surgió con la colocación de información falsa en boletines informativos o e-mails, por ejemplo, para beneficiarse de las inversiones dentro de la bolsa financiera. También pueden llevarse a cabo modificando información caduca. Esta generación de ataques se lleva a su extremo si se modifica el contenido de los datos de los programas, que son incapaces de sospechar de su veracidad, como por ejemplo la manipulación del sistema de control de tráfico aéreo, el control de un coche inteligente, la base de datos de los libros más vendidos o de índices bursátiles como el NASDAQ [50].

7.1 Escenarios De Vulnerabilidad Red WAN

Ingeniería Social: La ingeniería social es una debilidad enfocada a encontrar las falencias del factor humano en una organización, los atacantes saben cómo aprovechar dichas falencias para realizar sus actos delictivos. En la ingeniería social, los seres humanos representan un talón de Aquiles a la hora de buscar la manera de tener acceso a la información de una organización, puesto que a diferencia de los componentes electrónicos son un elemento manipulable capaz de romper las reglas establecidas en las políticas de seguridad de la información. Los atacantes se aprovechan del desconocimiento, negligencia o ignorancia de las personas para acceder a la información o generar el ataque en los sistemas informáticos de las organizaciones.

Factor Insiders: son agentes dentro del interior de una red en las organizaciones que se encargan de atacar sistemas informáticos. Comúnmente dichos agentes son los mismos empleados que posiblemente pueden estar dentro de la organización única y exclusivamente con la intención de hacer estragos. Por otro lado, también pueden ser empleados que debido a un disgusto, problema o conflicto con los demás, han decidido a manera de venganza hacer algún tipo de acto delictivo. Los Factor Insiders por su naturaleza de actuar dentro de la organización, son en gran medida inmunes a los sistemas de seguridad estándar que se aplican en las empresas, pues éstos van enfocados hacia el exterior.

Uso de Contraseñas: representan un elemento de seguridad clave para los atacantes o intrusos, pues la mayoría de sistemas informáticos requieren de una autenticación a los usuarios por medio de contraseñas. El uso de contraseñas para mantener la confidencialidad y la seguridad de los diferentes usuarios en la red, es una práctica de seguridad antigua pero aún hoy en día se mantiene vigente por su efectividad. La fortaleza de la contraseña se enfoca en que sea un código difícil de descifrar, que se mantenga en secreto. Sin embargo, esto hace que sea vulnerables a técnicas de ingeniería social.

Ejecución De Configuraciones Predeterminadas: Las configuraciones predeterminadas son un factor de fácil vulneración por parte de los intrusos y atacantes, puesto que los códigos maliciosos e intrusiones, son hechos pensando inicialmente en que el equipo o sistema a atacar se encuentra configurado de forma predeterminada. De esta forma el intruso puede sacar provecho del hecho de saber los parámetros y estándares que conforman dicha configuración. El Exploit es un tipo de código que se encarga precisamente en aprovechar las configuraciones predeterminadas de un equipo. También existen sitios web que contienen bases de datos con toda la información de usuarios, contraseñas, códigos de acceso, valores por defecto de los sistemas operativos, entre otros [50].

7.2 Agujeros de Seguridad WAN

7.2.1 Ataques a la Capa de Aplicación

DNS Spoofing: Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa.

SMTP Spoofing y Spamming: En un nivel superior, concretamente a nivel de aplicación, en el protocolo SMTP (puerto TCP 25) es posible falsear la dirección fuente de un correo o e-mail, enviando por tanto mensajes en nombre de otra persona. Es así porque el protocolo no lleva a cabo ningún mecanismo de autenticación cuando se realiza la conexión TCP al puerto asociado

DOS (Denial of Servicies): En los protocolos de los modelos TCP/IP y OSI, se analizan los ataques basados en la denegación de servicio (DoS) desde el exterior de un sistema, a través de la red, y no una vez se disponga de acceso de administrador en el mismo.

Si se tiene acceso a los dispositivos de red, éstos pueden re arrancarse o apagarse, con la implicación que tendría en las comunicaciones de la red de la organización afectada. Un ataque de denegación de servicio se centra en sobrepasar los límites de recursos establecidos para un servicio determinado, obteniendo como resultado la eliminación temporal del servicio [50].

7.2.2 Ataques a la Capa de Transporte

Los ataques a la capa de transporte van asociados al funcionamiento de los protocolos TCP y UDP. Escaneo de puertos, inundaciones UDP, DoS por sobrecarga de conexiones, son algunos de los ataques a dicha capa. A continuación, se detallan los ataques y vulnerabilidades con más nivel de detalle:

Fingerprinting: Una técnica que permite extraer información de un sistema concreto, es decir; la obtención de su huella identificativa respecto a la pila de protocolos. El objetivo primordial suele ser obtener el sistema operativo que se ejecuta en la maquina destino de la inspección. Esta información junto con la versión del servicio o servidor facilitara la búsqueda de vulnerabilidades asociadas al mismo. La probabilidad de acierto del sistema operativo remoto en muy elevada, y se basa en la identificación de las características propias de una implementación de la pila frente a otra, ya que la interpretación de los RFCs no concuerda siempre. Para poder aplicar esta técnica con precisión es necesario disponer de un puerto abierto (TCP y/o UDP).

Escaneo de Puertos: Una vez que se dispone de los dispositivos a nivel IP activos en una red (por ejemplo, mediante ICMP), puede aplicarse a cada uno de ellos una técnica, centrada en la posterior búsqueda de vulnerabilidades, basada en una exploración de escaneo de puertos abiertos, tanto UDP como TCP [50].

7.2.3 Ataques A La Capa De Red

La capa de red no está exenta de los ataques que usuarios o hackers efectúan contra las vulnerabilidades del modelo OSI. A continuación, se presentan los principales ataques

Footprinting: Para lograr hacer un ataque o un acceso indebido a algún sistema conectado por medio de redes, lo primero que se debe hacer es tener algunos datos relevantes con el fin de saber cuál es el camino que se debe seguir, por lo general este ataque es el primero que prueban los hackers para recopilar información sobre la red como: el Rango de la Red y Sub Red, los puertos abiertos y las aplicaciones que los utilizan. También saber el o los sistemas operativos que corren en los equipos, direcciones IP específicas entre otras.

Escaneo Basado en el Protocolo ICMP En todo sistema es necesario analizar los usos indebidos que se le pueden dar al escaneo de un sistema remoto, utilizando técnicas basadas en protocolos ICMP

IP Spoofing: Se basa en la generación de paquetes IP con una dirección de origen falsa, se puede hacer envío de paquetes con este tipo de direcciones para que desde la misma maquina se disponga de un sistema destino objetivo, porque existe un dispositivo de filtrado que permite el tráfico de paquetes con esta dirección de origen, o porque existe una relación de confianza entre esos dos sistemas [50].

7.2.4 Ataques A La Capa De Enlace De Datos

Los ataques a la capa de enlace de datos se centran en el protocolo ARP (Address Resolution Protocol), VLAN y en STP (Spanning Tree Protocol). A continuación, se mencionan:

ARP Spoofing: Es una técnica usada para infiltrarse en una red Ethernet conmutada (basada en Switch y no en Hubs), que puede permitir al atacante husmear paquetes de datos en la WAN, modificar el tráfico, o incluso detener el tráfico. El atacante envía mensajes ARP falsos o falsificados a la Ethernet, con la finalidad de asociar la dirección MAC del atacante con la dirección IP de otro nodo (nodo atacado), un ejemplo puede ser la puerta de enlace Gateway. Cualquier tráfico dirigido a la dirección IP de dicho nodo será enviada al atacante en vez de al destino original.

Switch Port Stealing (SNIFFING): Utilizando ARP Spoofing el atacante consigue que todas las tramas dirigidas hacia otro puerto del switch lleguen al puerto del atacante para luego re-enviarlos hacia su destinatario y de esta manera poder ver el tráfico que viaja desde el remitente hacia el destinatario.

VLAN Hopping Attack: Un equipo puede hacerse pasar como un Switch con 802.1Q/ISL y DTP, o bien se puede emplear un Switch. El equipo se vuelve miembro de todas las VLAN. Este ataque requiere que el puerto este configurado con el modo Trunking “automático” [50].

7.2.5 Ataques a la Capa Física

Los ataques a la capa física van enfocados a daños provocados en los dispositivos que pertenecen a la red. Desde una simple desconexión de cable UTP hasta un incendio provocado se puede considerar un ataque a dicha capa. Un ataque a los sistemas físicos de una red de comunicaciones puede ocasionar una sucesión de problemas que pueden incluso causar mayor impacto que los ocasionados en la parte lógica de la misma. [50].

Capítulo 7

8. Propuesta de Guía Metodológica Para la Implementación de Software Seguro y Protocolos de Seguridad en Sistema de Redes de Datos

Un principio básico de la ingeniería de software es que no se puede controlar lo que no se puede medir. Las pruebas de seguridad no son ajenas a este concepto Por desgracia, la medición de la seguridad es un proceso muy difícil, que requiere de un previo conocimiento al momento de interpretar y tomar cualquier tipo de decisión, que no afecte los intereses económicos de la empresa

Un aspecto que hay que resaltar es que las mediciones de seguridad se realizan sobre los aspectos técnicos específicos (por ejemplo, vulnerabilidades) y decisiones que afectan a la economía del software, Si bien la estimación del coste de software inseguro puede parecer una tarea de enormes proporciones, pero estudios anteriormente mencionados difieren que la implementación de este tipo de software Para el desarrollo de esta propuesta metodológica se tendrán en cuenta diversos aspectos como la revisión de la política de seguridad de la información y la organización, luego se tendrá en cuenta la evaluación de riesgos para la implementación de software seguro, posteriormente se evaluaran aspectos como la seguridad física, controles técnicos e ingeniería social, por último se detallara los requerimientos legales y regulatorios que comprenden y son de suma importancia en el desarrollo de software seguro en las redes de datos, cabe mencionar que para implementar software seguro no solo se necesitara conocer de seguridad en el desarrollo de este, si no que se tendrán en cuenta otros aspectos que son importantes dentro del entorno.

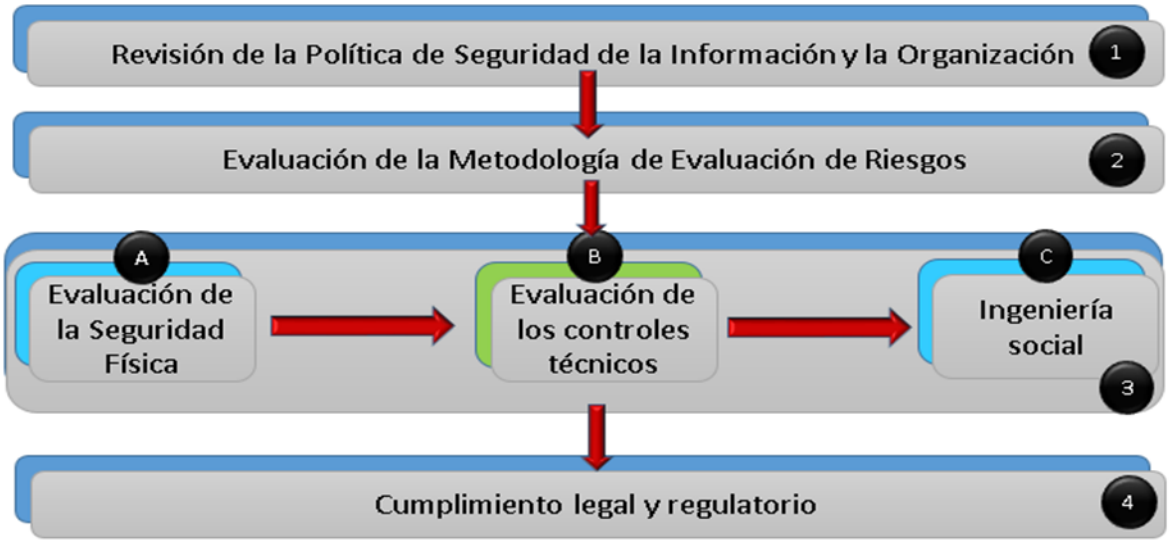


Figura 19. Marco De Evaluación De La Seguridad En Sistemas De formación

8.1 Paso 1 - Revisión de la Política de Seguridad de La Información y Organización

Una política de seguridad de la información y organización a menudo determinan la eficacia de la aplicación de seguridad dentro de una empresa. Una política de información y una organización van de la mano para garantizar seguridad, éstos pueden ser tratados como los componentes básicos del programa de seguridad de la información. Mientras que la política de seguridad es una declaración que se deriva de los requisitos de negocio de la organización garantizando que estas declaraciones se apliquen eficazmente.
En este primer paso se tendrán en cuenta aspectos que son necesarios como: cuales son los requisitos que deberán tener los usuarios de esta política en dicha organización, cuales son las restricciones para manejar la información y cuáles son las funciones de los encargados del departamento de T.I que es el organismo encargado de hacer cumplir estas funciones

8.1.1 Tarea A1 - Verificación de Seguridad en la Organización

La organización de seguridad juega un papel vital en la aplicación efectiva y general de la seguridad de una empresa. La mayoría de las empresas en general tienen seguridad de la información alineado con el departamento de TI. El alcance de la seguridad de la información es mucho más amplio que sólo la seguridad de TI, ya

que implica una gran cantidad de interacción con otros departamentos de la empresa. Por tales razones en su mayor capacidad tienen la seguridad de la información alineado con el Departamento de Operaciones.
En la situación más ideal de la Organización de Información de Seguridad debe ser directamente dependiente del jefe de la oficina ejecutiva de la compañía. Esto no siempre puede ser posible y en tales escenarios la organización de seguridad de la información podría ser dependiente del ejecutivo responsable del desarrollo, implementación y operación de la política de tecnología de la información de una empresa.

Dentro de esta política de organización de la seguridad encontramos varias referencias que se deben tener en cuenta como, por ejemplo:

- **Declaración de Gestión de Seguridad de Información:** Esta declaración deberá incluir el compromiso de la gestión y soporte de seguridad de la información dentro de la organización. Esto también animará a otras unidades de negocio para participar en el programa de seguridad de la información para la empresa.

- **Declaración disciplinaria:** La política debe incluir una declaración, que debería hablar sobre el proceso disciplinario que deberá producirse en caso de que haya un incumplimiento de las políticas mencionadas a continuación. Las medidas disciplinarias pueden ser hasta la terminación del empleo.

- **La organización de seguridad, los roles y responsabilidades:** Esta sección debe incluir los diferentes roles en el programa de seguridad de la información. Esto debería incluir como mínimo el papel del Oficial de Seguridad de la Información, los dueños de la información, los usuarios finales, el administrador de sistemas y los usuarios finales.

8.1.2 Tarea A2 - Identificación de Usuarios Finales

- **Uso Aceptable de los Sistemas y Recursos de Computación:** Esta política habla de cómo los sistemas de información son importantes para la organización y También sobre el uso prudente de los sistemas informáticos por parte de los empleados. La mayoría de las organizaciones tienen una política que define que todos los datos almacenados en los sistemas informáticos pertenecen a la organización y que la actividad de los empleados puede ser monitoreada.

- **Política de uso E-mail:** Esta política se habla del uso prudente de los recursos de correo electrónico. Esto significa que los empleados pueden utilizar el sistema de correo electrónico para uso personal, siempre y cuando no haya un uso significativo del ancho de banda de la organización.

- **Uso de Internet:** El uso de Internet se concede principalmente a los empleados que requieren acceso para fines comerciales. También se recomienda a los empleados contra la publicación de cualquier comentario sobre los sitios web con la empresa Identificación del correo electrónico menos que esté autorizado para hacerlo.

- **Cifrado de datos sensibles:** Se debe advertir a los empleados lo importante de cifrar la información sensible antes de ser enviada a través de Internet. También deben confirmar la identidad de los remitentes y asegurarse de que es de una fuente auténtica antes de utilizar la información enviada a los usuarios.

- **Política Anti-Malware:** La política anti-malware debe aconsejar a los usuarios sobre el escaneo de archivos adjuntos antes de obtener a partir de fuentes externas. También deben reportar los incidentes de virus a las personas interesadas que podrían ayudar en la contención de los virus / gusanos antes de que comienza a expandirse a otros sistemas.

8.1.3 Tarea A3 – Que Deben Hacer los Propietarios de la Información

- **Evaluación de Riesgos y clasificación de activos:** deberá ser realizado por la evaluación del riesgo y la clasificación de los sistemas de información en su ámbito de competencia. Ellos, junto con los representantes forman el departamento de seguridad de la información donde se debe clasificar y etiquetar los datos mediante el análisis de las amenazas.

- **Proveedores De Servicios Externos Política De Compromiso:** Los propietarios de la información deben notificar al departamento de seguridad de la información acerca de los posibles compromisos con proveedores de servicios externos antes de establecer una relación. El departamento de seguridad de la información debe analizar si los proveedores de servicios cumplen con los criterios mínimos necesarios para que los datos de las organizaciones puedan ser confiados.

8.1.4 Tarea A4 - Políticas Para El Departamento De T.I

- **Seguridad Física de los Sistemas de Información:** Esta política debe asesorar al Departamento de TI o de otros departamentos (administración) para desplegar todos los posibles controles de seguridad para proteger los sistemas de información de los daños, la pérdida y el robo de la información

- **Sistemas de Red y Política de Seguridad:** Se encarga de discutir los mecanismos de seguridad que se aplicarán en los sistemas de servidores de red y. Los principales criterios para la configuración de los sistemas que deben acceder a los recursos según sea necesario.

- **Seguridad inalámbrica:** Esta es un área que es un motivo de grave preocupación. Los sistemas inalámbricos se deben configurar correctamente con métodos de autorización y autenticación adecuadas.

- **Conectividad a Internet:** Esta política debe hablar de una conectividad segura a Internet y terceros. El método aceptable para las organizaciones de la conectividad externa y el proceso de autorización para el mismo debe ser discutido. Algunas organizaciones llevan a cabo una prueba de penetración en las redes de terceros antes de permitir la conectividad en sus sistemas.

- **Política de compromiso proveedor:** La política de compromiso proveedor se enfoca en qué el criterio mínimo de seguridad de un vendedor debe verificarse antes de ejecutarse en la organización, para establecer una relación, Por ejemplo, un vendedor incluye una adecuada verificación de antecedentes de todos sus empleados antes de que los proveedores de representantes trabajen con la organización.

- **Política de disponibilidad de copia de seguridad y sistemas:** Esta política hace referencia al buen funcionamiento de la infraestructura de red y de la seguridad de los sistemas de información para el departamento de T.I.

8.1.5 Tarea A5 – Requerimientos de la Seguridad de la Información

- **Monitoreo y reseña de eventos de seguridad del sistema:** El equipo de seguridad de la información debe ser aconsejado para comprobar los eventos de seguridad de forma regular e informar infracciones o incidentes graves en la naturaleza de la gestión. El equipo de seguridad de la información debe vigilar periódicamente por cualquier incumplimiento de la política de seguridad y así trabajar con las unidades de negocio para tener control sobre ello.

- **Sistemas de evaluación de la vulnerabilidad y pruebas de penetración:** El departamento de seguridad de la información es a menudo el encargado de llevar a cabo pruebas de evaluación de la vulnerabilidad y de penetración. Esta política habla de cómo éstos estándares deben llevarse a cabo con la debida autorización.

- **Respuesta al incidente:** La política de respuesta a incidentes detalla el método de investigación de las violaciones de seguridad reportados. ¿Cómo y cuándo los organismos encargados de hacer cumplir la ley y quien debe ser responsable de la emisión de información con los medios de comunicación?

- **Temas de seguridad y capacitación:** Este es un tema a menudo se pasa por alto; el departamento de seguridad de la información debe ser responsable de la formación de todos los usuarios en las organizaciones. También deben diseñar y actualizar constantemente sus programas de sensibilización de seguridad

8.2 Paso 2 - Evaluación de la Metodología de Evaluación de Riesgos

Se delimita como el potencial de las pérdidas sufridas debido a un evento indeseable y debe ser un producto de la amenaza X Valor de activos a los activos de X vulnerabilidades. Para encontrar el riesgo total y asignar una puntuación determinada los otros factores deben ser conocidas estas amenazas.

8.2.1 Tarea B1 - Valor de Activos

puede ser conocido a través de un ejercicio de valoración de activos. En primer lugar, los procesos claves del negocio y los activos de información que complementan estos procesos deben ser identificados. Estos activos en la mayoría de los casos tendrán la puntuación más alta que a su vez indica su importancia o criticidad de la organización. Los activos también pueden evaluarse para determinar los elementos tangibles, como la pérdida financiera y los impactos regulatorios, junto con factores intangibles como la pérdida de la confianza del cliente. El valor de los activos dependerá de:

- Costo de producción de la información
- Valor de la información en el mercado abierto
- Costo de reproducción de la información si se destruye
- Repercusión de la empresa si la información no estaba disponible
- Ventaja que daría a un competidor si podían usar, modificar, o destruir la información
- Coste para la empresa si la información fue puesta en riesgo, alterada o destruida
- La pérdida de la confianza del cliente o cliente si la información no se llevó a cabo y se procesa de forma segura

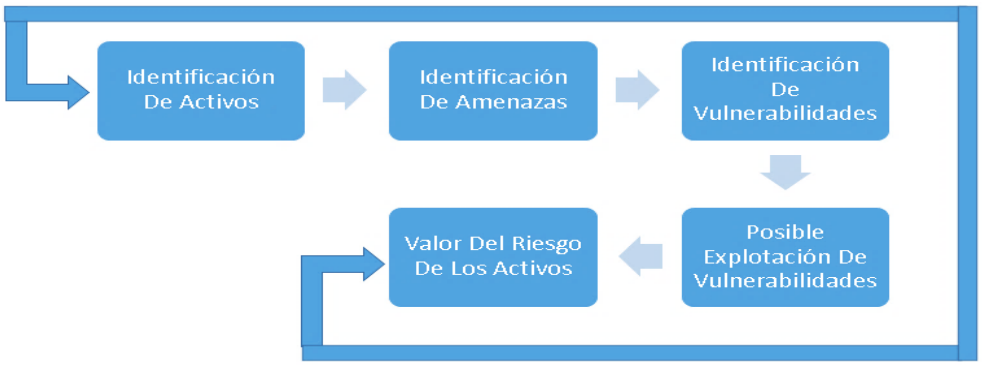


Figura 20. Procesos De Evaluación De Riesgos

8.2.2 Tarea B2 - Identificación De Activos

Esta fase se encarga de priorizar y clasificar la información que queremos que sea objeto de análisis, un ejemplo de la identificación de activos seria:

- Activos de información (datos, de manuales de usuario, entre otros)
- Documentos en papel (contratos)
- Activos de software (aplicación, software de sistemas, entre otros)
- Activos físicos (computadoras, servidores, medios magnéticos, enrutadores, entre otros)
- Personal (estudiantes, clientes, empleados, entre otros)
- Imagen de la compañía y reputación
- Servicios (comunicaciones, entre otros)

8.2.3 Tarea B3 - Identificación De Amenazas

Una amenaza es la existencia de algún mecanismo, que activado, permite explotar una vulnerabilidad. Una amenaza para poder causar daño a un activo debe estar asociada a una vulnerabilidad en el sistema, aplicación o servicio.

- **Identificación de vulnerabilidades**: una vulnerabilidad es un error que representa un problema potencial, es decir, es una condición de debilidad, que le permite a una amenaza producir un daño en la organización.
- **Posible Explotación De Vulnerabilidades**: una amenaza para poder causar algún tipo de daño a un activo, tendría que explotar la vulnerabilidad del sistema, aplicación o servicio. Las vulnerabilidades son condiciones que pueden permitir que las amenazas las exploten y causen daño.
- **Valor Del Riesgo De Los Activos:** se realiza la clasificación cuantitativa, asignándole un valor a los activos, dependiendo del grado de comprometimiento, un ejemplo de la asignación de estos valores podría ser:

    - Riesgo alto 5 puntos
    - Riesgo medio: 3 puntos
    - Riesgo Bajo 2 puntos
    - Alertas: 1 punto

8.3 Paso 3 - Evaluación De La Seguridad Fisica

Garantiza que el acceso a los sistemas de hardware y otros elementos vitales para los sistemas que funcionan como el servicio de energía eléctrica, el aire acondicionado y calefacción central, líneas telefónicas y de datos, medios de copia de seguridad y documentos de origen se controlan adecuadamente. Esto también garantiza el mantenimiento de un entorno adecuado para el funcionamiento óptimo de sistemas estos sistemas

Protección contra Incendios
Se requiere un equipo de detección de incendios para detectar rápidamente un fuego y extinguirlo. También es importante determinar con precisión la ubicación del incendio.

Proceso

- Sistemas de detección de incendios
- Equipo de supresión de incendios
- Extintores

8.3.1 Tarea C1 - Ingeniería Social

Son los métodos más simples para obtener información sin tener que comprometer las herramientas de seguridad implementados en el sistema de información.

La mayoría de los sistemas de información dependen de un cierto nivel de confianza para su funcionamiento. Por ejemplo, las grandes organizaciones dependen en gran medida de correo electrónico y acceso remoto para la comunicación y, a menudo todos los usuarios se les asignan contraseñas de identidad para su acceso. En caso de que los usuarios colocan mal sus contraseñas tienen la flexibilidad de llamar al departamento de TI y conseguir cambiar sus contraseñas. Cuando un usuario llama al departamento de TI para restablecer el acceso, hay un cierto nivel de confianza que se establece entre el usuario y el analista de asistencia. Un hacker intenta crear esta confianza para obtener información valiosa del analista de asistencia [51].

8.4 Paso 4 – Identificación del Cumplimiento legal y Regulatorio

Hace referencia a todo el marco legal que debe adoptar la empresa al momento de ejercer el cumplimiento de todas las políticas internas y externas que estén relacionadas con dicha entidad. Deben cumplir con los estándares internacionales y nacionales, algunos de los estándares y normativas internacionales son la serie ISO/IEC 27000 y los criterios comunes.

8.5 Paso 5 - Políticas de Seguridad para Sistema de Redes de Datos

8.5.1 Tarea D1 - evaluación De La Seguridad WLAN

Gestión dela Clave

- Pre claves compartidas son las formas tradicionales de hacer un intercambio de claves en redes de área local inalámbricas.
- Intercambio de claves es dinámico protocolos tales como 802.1x, que permite a las llaves ser compartidos de forma dinámica.
- Posibilidad de exposición o el robo de claves de cifrado estáticas almacenada en los puntos de acceso y las estaciones inalámbricas.

Cifrado

Las redes inalámbricas no tienen restricción de la conectividad física. El estándar IEEE 802.11 especifica WEP como el equivalente inalámbrico a la seguridad física proporcionada por las redes cableadas. El esquema de cifrado WEP utiliza claves compartidas para el cifrado y descifrado de los marcos pasaron a través de una LAN inalámbrica (WLAN).

WEP también puede ser descubierto en un corto período de tiempo. Aunque WEP se basa en el robusto algoritmo de clave simétrica RC4, las fallas en la implementación de WEP han sido bien documentados. Estos defectos permiten que un usuario malintencionado que se acumula suficiente WEP marcos cifrados en red dada para identificar los valores compartidos entre los marcos y en última instancia, determinar la clave compartida.

WPA y WPA2 requieren que los usuarios proporcionen una clave de seguridad para conectarse. Una vez que se ha validado la clave, se cifran todos los datos intercambiados entre el equipo o dispositivo y el punto de acceso.

Existen dos tipos de autenticación WPA: WPA y WPA2. Si es posible, use WPA2 porque es el más seguro. Prácticamente todos los adaptadores inalámbricos nuevos son compatibles con WPA y WPA2, pero otros más antiguos no. En WPA-Personal y WPA2-Personal, cada usuario recibe la misma frase de contraseña. Éste es el modo recomendado para las redes domésticas. WPA-Enterprise y WPA2-Enterprise se han diseñado para su uso con un servidor de autenticación 802.1x, que distribuye claves diferentes a cada usuario. [52].

Recopilación de información

Puntos de acceso inalámbricos y los clientes las emisiones, respectivamente. son enviados por los puntos de acceso a intervalos predefinidos. Son invitaciones e instrucciones de conducción que permiten al cliente encontrar el punto de acceso y configurar los valores adecuados para comunicarse.

Exploración

- Detectar e identificar la red inalámbrica
- Test de canales y ESSID
- Prueba de la trama de baliza de emisión y registro de información de difusión
- Prueba de puntos de acceso no autorizados desde fuera de la instalación
- Colección de direcciones IP de los puntos de acceso y clientes
- Recolección de direcciones MAC de los puntos de acceso y clientes
- Detectar e identificar la red inalámbrica

Auditoria

- Controles de implementación
- Control de acceso
- El control de acceso puede estar basada en la dirección de MAC de los dispositivos de conexión.
- La configuración del firewall
- Puertos en el dispositivo

8.6 Paso 6 - Evaluación de Dispositivos de Red

Antes de decidirnos a implementar el software seguro, en un sistema de redes de datos, debemos realizar un análisis y evaluación de los principales dispositivos que componen un sistema de redes de datos WAN

8.6.1 Tarea E1 - Evaluación De La Seguridad Del Switch

En el Switch de seguridad de capa 2. Se realizan pruebas de seguridad integral. Un agujero es suficiente para exponer la seguridad a la LAN corporativa. Un atacante no necesita para atacar a la capa más alta si la capa inferior puede dar acceso a él.

Ataques de suplantación del Switch

La suplantación de identidad de Switch es un tipo de ataque con salto de VLAN que funciona mediante el aprovechamiento de un puerto de enlace troncal mal configurado. De manera predeterminada, los puertos de enlace troncal tienen acceso a todas las VLAN y pasan el tráfico para varias VLAN a través del mismo enlace físico, generalmente entre Switches.

En un ataque de suplantación de identidad de Switch básico, el atacante aprovecha el hecho de que la configuración predeterminada del puerto del Switch sea dinámica automática. El atacante de la red configura un sistema para suplantar su propia identidad y hacerse pasar por un Switch. Esta suplantación de identidad requiere que el atacante de la red pueda emular mensajes. Al hacerle creer al Switch que otro Switch intenta crear un enlace troncal, el atacante puede acceder a todas las VLAN permitidas en el puerto de enlace troncal.

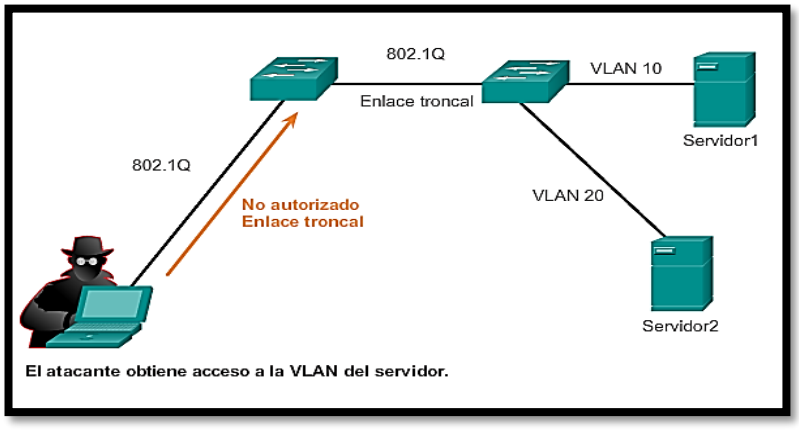


Figura 21. Ataque de suplantación de identidad del Switch[53]

Como prevenirlo

La mejor manera de prevenir un ataque de suplantación de identidad de Switch básico es inhabilitar los enlaces troncales en todos los puertos, excepto en los que específicamente requieren enlaces troncales. En los puertos de enlace troncal requeridos, inhabilite Protocolo de enlace troncal dinámico y habilite los enlaces troncales manualmente.

8.6.2 Tarea E2 - Evaluación De La Seguridad Del Router

Identificar el nombre de host del Router

Identificar el nombre de host del Router solo se hace para propósitos informativos solamente y no es necesario que escriba las direcciones IP todo el tiempo. Si el Router se ha registrado en el DNS, una consulta inversa de la dirección IP del Router le dará el nombre DNS del Router. Este nombre DNS podría ser el mismo que el nombre de host.

Detección de sistema operativo

Encontrar el sistema operativo y versión del dispositivo del enrutador permite a atacantes probadores / penetración para encontrar vulnerabilidades específicas y posible intrusión. Los resultados esperados son el tipo y versión del sistema operativo del Router.

VTY Prueba / Conexiones

La forma más sencilla y directa para conectarse al dispositivo de red es utilizar una conexión directa con el puerto de consola. Conexiones VTY. se utilizan para conectar un terminal directamente en el Router, y la configuración por defecto del enrutador sin seguridad es aplicada al puerto de consola. También la utilidad de configuración no solicita administrador permisos para configurar la seguridad de acceso a la consola.

Como prevenirlo

- No utilice telnet para la gestión remota de los Routers
- Utilizar listas de control de acceso adecuadas para conexiones de administración remota
- Coloque mecanismo de control de acceso en todas las líneas terminales
- Implementar mecanismos de control de acceso basado en el usuario

Activar el registro

Configurar el registro y la supervisión de los registros sobre una base regular. El análisis de los registros identificará actividades maliciosas y proporcionar señales de alerta temprana
El escaneo del router externo generalmente no es detectado por un sistema de detección de intrusiones de red. Se recomienda que ingrese.
También los paquetes que se filtra por las listas de control de acceso generalmente no son detectados por un sistema de detección de intrusiones de red. Se recomienda que ingrese.

Limitar el acceso de Telnet

Los Router pueden ser gestionados de forma remota a través de una conexión Telnet. Es una buena idea para limitar, o incluso inhabilitar el acceso de Telnet. Permitir la administración del puerto de consola. Si se requiere una gestión remota limitar el acceso a determinadas direcciones IP.

Proteger las contraseñas

Proteger las contraseñas en el sistema con MD5 o algoritmo hash equivalente. En caso de contraseñas, donde la opción no está disponible para el uso de cifrado codificar cadenas de contraseña

Configurar el filtrado de ingreso

Para protegerse de los intrusos o los usuarios no sean de confianza en la red interior, utilizar Ingress Filtering. Al negar los paquetes con direcciones de origen simuladas de la red interna, el filtrado de entrada impide que usuarios maliciosos dentro de lanzar algunos ataques de denegación de servicio (DoS)

8.6.3 Tarea E3 - Evaluación de la Seguridad del Servidor

Analizar los problemas de seguridad a nivel del sistema operativo y de las aplicaciones de los entornos operativos de su empresa. verificar los controles administrativos y técnicos, identificado debilidades potenciales y reales y recomienda contramedidas específicas.

Las Evaluaciones de la configuración de seguridad del servidor son fundamentales porque nos permiten identificar vulnerabilidades que no se pueden detectar a través

de evaluaciones de la red. Estas evaluaciones son el mecanismo más eficaz para evaluar de manera completa la seguridad de los activos críticos de su organización.

llevar a cabo Evaluaciones de la configuración de seguridad del host para entornos Microsoft Windows y UNIX, incluyendo aplicaciones importantes como IIS, SQL Server y Apache. También realizar evaluaciones de la configuración de seguridad del host para sistemas en entornos de producción, incluidos servidores Web de comercio electrónico, bases de datos financieros y hosts de defensa orientados a Internet

8.7 Paso 7 - Desarrollo e Implementación de Aplicaciones o Software

El desarrollo y la implementación de políticas de aplicaciones debe hablar sobre cómo la seguridad debe ser considerada en el momento de implementar aplicaciones o software. La política también debe discutir los medios en los que la aplicación se debe probar, ejecutándola en un entorno de integración y sólo después de que pase las pruebas de seguridad y requisitos anteriormente mencionados en, se deben implementar en los sistemas de producción.

En este caso se recomienda la instalación de un firewall tipo software que permita detener y controlar todas las vulnerabilidades existentes en nuestra red, pero antes se realizara un análisis de cómo se debe realizar la evaluación de seguridad de este software.

8.7.1 Tarea E1- Evaluación de Seguridad de Firewall

Identificación de las aplicaciones

- Confirmación de que el dispositivo puede identificar diversas aplicaciones. La mejor forma de comprobarlo es instalando el firewall en modo transparente en la red.
- Confirmación de que el dispositivo puede identificar el tráfico de aplicaciones tanto con herramientas de visibilidad y análisis de alto nivel como con herramientas de bajo nivel.
- Evaluación de los pasos a dar para habilitar la identificación de aplicaciones por primera vez. ¿Cuánto se tarda en establecer una política y empezar a “ver” el tráfico de aplicaciones? ¿Es preciso dar algún otro paso para aumentar la

visibilidad de las aplicaciones que cambian de puerto o usan otros alternativos?

Identificación de las aplicaciones que cambian de puerto o usan otros alternativos

- Verificación de que el firewall es capaz de identificar y controlar aplicaciones que entren por puertos distintos a los que tienen asignados por omisión. Por ejemplo, SSH por el puerto 80 y Telnet por el puerto 25.
- Confirmación de que el firewall es capaz de identificar aplicaciones que pasan de un puerto a otro gracias a aplicaciones como Skype, AIM o aplicaciones P2P.

La identidad de las aplicaciones ha de ser la base de la política de firewall

- Confirmación de que al crear la política de firewall se toma la aplicación y no el puerto como elemento principal. En otras palabras, ¿requiere la política de control de aplicaciones de alguna norma basada en puertos? ¿Es el controlador de las aplicaciones un editor de políticas separado?
- Creación de una política para permitir algunas aplicaciones y bloquear otras y verificación de que las aplicaciones son controladas como cabe esperar.

8.8 Paso 8 - Cómo Implementar Un Firewall De Nueva Generación

Administración

- Se ha de analizar la complejidad administrativa del dispositivo en pruebas y la dificultad (pasos a dar, claridad de la interfaz, etc.) de la tarea a realizar.
- Confirmación de la metodología administrativa del dispositivo en pruebas. ¿Se necesita otro servidor para la administración individual de cada dispositivo? ¿Se puede administrar a través de un navegador o se necesita un cliente pesado?
- Comprobación de la disponibilidad de las herramientas de visualización mediante el repaso de las aplicaciones, amenazas y direcciones URL de la red.
- Comprobación de que los controles de seguridad de aplicaciones, controles de firewall y funciones preventivas se pueden habilitar desde un mismo editor.

8.8.1 Tarea F1 - Evaluación del Rendimiento con los Servicios Habilitados

El control de las aplicaciones conlleva una carga de recursos mucho mayor que la propia de un firewall basado en puerto tradicional, por lo que es esencial comprobar que el dispositivo en pruebas rinde convenientemente durante la identificación y el control de las aplicaciones.

- Comprobación del producto: software, servidor o dispositivo integrado.

- Investigación de la arquitectura del hardware, si se trata de un dispositivo, para confirmar que se aplica la capacidad de procesamiento adecuada para la tarea a realizar. El uso de servidores multifuncionales limita el rendimiento de la red al habilitar los servicios de seguridad.

- Evaluación del rendimiento en un entorno de pruebas que se asemeje al entorno definitivo del sistema. [54]

9. Conclusiones

Cuando se decide realizar la implementación del software, se debe tener en cuenta diferentes aspectos como el ciclo de vida del desarrollo del mismo, debido a que la corrección de algún defecto luego de que este haya sido implementado, puede resultar costoso para las organizaciones, y ocasionar retrasos en los procesos internos.

Es necesario tener políticas de seguridad que sean claras, sencillas y fáciles de implementar, pero a su vez que se adapten a las normas y estándares internacionales, y que permitan controlar y detener amenazas en cualquier sistema de redes de datos, utilizando técnicas como el escaneo de puertos y análisis de vulnerabilidades con herramientas de software y hardware.

En los procesos de implementación de software seguro en un sistema de redes de datos WAN, no solo se debe tener en cuenta los entornos físicos y las características del tipo de red donde este va a ser ejecutado, sino también una serie de procedimientos y procesos que involucran principalmente al recurso humano que es el que está a cargo del control, manipulación y corrección de las posibles vulnerabilidades.

En la actualidad existen muchas herramientas que permiten la detección de amenazas, pero hasta el momento por temas comerciales aún no se ha creado un software, aplicación que contenga en su estructura un algoritmo que le permita ejercer control, a su vez que se actualice, de tal forma que le permita la detección completa de malware o códigos maliciosos.

Existen muchas metodologías que se enfocan en el desarrollo de software seguro, esta guía metodológica se basa en muchos conceptos de metodologías como la OWASP, OSSTMM, e ISSAF que permitieron ver una perspectiva y orientarla a los sistemas de redes de datos y más específicamente a los sistemas de redes WAN.

10. Referencias

[1] "ISECOM - Instituto de Seguridad y Metodologías Abiertas." [Online]. Available: http://www.isecom.org/. [Accessed: 23-Nov-2015].

[2] Universidad Nacional Abierta y a Distancia, "Lección 29 ISSAF," 2015. [Online]. Available: http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_29_issaf.html. [Accessed: 23-Nov-2015].

[3] "OWASP Top 10 Privacy Risks Project - OWASP." [Online]. Available: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project#tab=Main. [Accessed: 21-Nov-2015].

[4] "ISO/IEC 27000:2014(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary." [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en. [Accessed: 21-Nov-2015].

[5] "ISO/IEC TR 20004:2012(en), Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045." [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:20004:ed-1:v1:en. [Accessed: 13-Nov-2015].

[6] "La detección de malware a nivel mundial crece un 40% en el primer trimestre de 2015 - Silicon News." [Online]. Available: http://www.siliconnews.es/2015/05/29/la-deteccion-de-malware-a-nivel-mundial-crece-un-40-en-el-primer-trimestre-de-2015/. [Accessed: 18-Nov-2015].

[7] "virus y males ciberneticos de las empresas colombianas - Dinero.com." [Online]. Available: http://www.dinero.com/empresas/articulo/virus-males-ciberneticos-empresas-colombianas/199331. [Accessed: 18-Nov-2015].

[8] C. Andrés R. Almanza, Msc, "XIII Jornada de Seguridad Informática," *ACIS (Asociacion Colombiana de Ingenieros de Sistemas)*, 2013. [Online]. Available: http://52.0.140.184/typo43/index.php?id=2057. [Accessed: 20-Nov-2015].

[9] soluciones tecnologicas. Funziona, "Seguridad en la red de la empresa," *2015*. [Online]. Available: http://www.funziona.com.ar/seguridad_red.php. [Accessed: 07-Dec-2015].

[10] RSA, "Phishing Kits – the Same Wolf, Just a Different Sheep's Clothing," no. February, 2013.

[11] J. L. Hernandez-Ardieta, "Ingeniería de Software Seguro | Indra," *2012*. [Online]. Available: http://www.indracompany.com/pt-br/ingenieria-de-software-seguro. [Accessed: 20-Nov-2015].

[12] R. Alder, J. Burke, C. Keefer, A. Orebaugh, L. Pesce, and E. S. Seagren, *How to Cheat at Configuring Open Source Security Tools*. Elsevier, 2010.

[13] D. Camacho Moreno, "Evaluaciones de seguridad en entornos TIC :

Fundamentos, metodologías y herramientas." Universitat Oberta de Catalunya.
[14] O. A. Acosta Naranjo, "Análisis de Riesgos y Vulnerabilidades de la Infraestructura Tecnológica de la Secretaría Nacional de Gestión de Riesgos utilizando Metodologías de Ethical Hacking." QUITO/EPN/2013, 26-Mar-2013.
[15] G. Erdogan, P. Meland, and D. Mathieson, "Security testing in agile web application development-a case study using the east methodology," *Agil. Process. Softw. …*, 2010.
[16] F. K. / A. ALONSO, "V. REDES DE TELECOMUNICACIONES," *2012*. [Online]. Available: http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm. [Accessed: 24-Nov-2015].
[17] "Redes de Datos y Conectividad," *2011*. [Online]. Available: http://personales.unican.es/zorrillm/MaterialOLD/redes.pdf. [Accessed: 24-Nov-2015].
[18] W. A. Network, U. Wan, L. Wan, and L. Lan, "CAPITULO I – ' Introducción a las redes WAN ,'" *CCNA*, vol. 4.
[19] Community Foundation International, "¿Qué es una aplicación web?," 2015. [Online]. Available: http://www.gcfaprendelibre.org/tecnologia/curso/informatica_basica/aplicaciones_web_y_todo_acerca_de_la_nube/1.do. [Accessed: 24-Nov-2015].
[20] "¿Qué es un firewall? - Ayuda de Windows." [Online]. Available: http://windows.microsoft.com/es-xl/windows/what-is-firewall#1TC=windows-7. [Accessed: 07-Dec-2015].
[21] J. Laskowski, *Agile IT Security Implementation Methodology*, vol. 22. Packt Publishing Ltd, 2011.
[22] D. "Applications E. by PKI", "Applications Enabled by PKI," *2011*. [Online]. Available: http://www.dartmouth.edu/~deploypki/materials/modules/applications/appsmenu.htm. [Accessed: 19-Nov-2015].
[23] E. R. Trujillo Machado, "Diseño e implementación de una VPN en una empresa comercializadora utilizando IPSEC." QUITO/ EPN/ 2006, 01-Mar-2011.
[24] F. López Provencio, "Desarrollo dirigido por la seguridad." Universitat Politècnica de Catalunya, 27-Jan-2015.
[25] G. Toth and J. Sznek, "Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM," p. 72, 2014.
[26] M. A. Mendoza and P. J. Moreno Patiño, "Desarrollo de una propuesta metodológica para determinar la seguridad en una aplicación web." Facultad de Ingenierías Eléctrica, Electrónica y Ciencias de la Computación, 2011.
[27] "2.4 Lección 9: Integración del SGSI (ISO 27001) a ISO 9001 –- 14000." [Online]. Available: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/24_leccin_9__integracin_del_sgsi_iso__27001_a_iso_9001__14000.html. [Accessed: 19-Ene-2016].

[28] “ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información.” [Online]. Available: http://iso27000.es/iso27002_8.html. [Accessed: 21-Feb-2016].
[29] “MODELO PARA LA EVALUACION EN SEGURIDAD INFORMÁTICA A PRODUCTOS SOFTWARE, BASADO EN EL ESTÁNDAR ISO/IEC 15408 COMMON CRITERIA,” *2011*. [Online]. Available: https://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/67925/1/modelo_evaluacion_seguridad.pdf. [Accessed: 22-Ene-2016].
[30] I. Cisco Systems, *Redes Cisco*. USERSHOP, 2010.
[31] “redes wan - 7.Topologias de Redes WAN.” [Online]. Available: https://redes-wan.wikispaces.com/7.Topologias+de+Redes+WAN. [Accessed: 06-Ene-2016].
[32] “Tecnologías de redes WAN y Frame relay | Informática y Telecomunicaciones | Xuletas, chuletas para exámenes, apuntes y trabajos.” [Online]. Available: https://redes-wan.wikispaces.com/7.Topologias+de+Redes+WAN. [Accessed: 06-Ene-2016].
[33] “Weitzenfeld: Capítulo 3,” *2014*. [Online]. Available: http://ftp.itam.mx/pub/alfredo/OBJETOS/MINT/Cap3-Procsw.pdf. [Accessed: 24-Ene-2016].
[34] P. Herzog, “OSSTMM 3.0 - The Open Source Security Testing Methodology Manual,” *Isecom*, p. 213, 2010.
[35] O. Foundation, “Guía de pruebas OWASP v3.,” vol. 0, p. 372, 2008.
[36] C. Commons, “OWASP Top 10 2013 Los Diez Riesgos Más Críticos en Aplicaciones Web,” p. 22, 2013.
[37] D. P. Valenzuela, *Software Libre y Software Propietario: Impacto Jurídico, Económico y Cultural en Colombia*. U. Externado de Colombia, 2013.
[38] “SOFTWARE LIBRE Vs. SOFTWARE LICENCIADO.” [Online]. Available: http://cdtiuniajc.blogspot.com.co/2013/03/programa-coti-21-marzo-2013.html. [Accessed: 24-Feb-2016].
[39] “Utilización Driftnet - System Security-ITC.” [Online]. Available: http://systemsecurity-itc.blogspot.com.co/2013/05/utilizacion-comando-driftnet.html. [Accessed: 24-Feb-2016].
[40] C. V. MIRANDA, *Sistemas informáticos y redes locales*. Ediciones Paraninfo, S.A., 2005.
[41] “FortiGuard® Antivirus Service | Fortinet.” [Online]. Available: http://www.fortinet.com/products/fortiguard/antivirus.html. [Accessed: 04-Feb-2016].
[42] “Nuevo Panda Antivirus 2016.” [Online]. Available: http://www.pandasecurity.com/security-promotion/Default.asp?reg=CO&lang=es&coupon=302520STDOFFER&track=99829&gclid=CjwKEAiAgeW2BRDDtKaTne77ghgSJACq2U4b57pBdKt3eISXcUT1NEyRnklqeEIMXloL1HdHb1m5jhoCW9Hw_wcB. [Accessed: 04-Feb-2016].

[43] “Descargar Antivirus Gratis - Avira Free Antivirus.” [Online]. Available: http://www.avira.com/es/avira-free-antivirus. [Accessed: 04-Mar-2016].
[44] “Como trabaja la Tecnología Antivirus de BitDefender.” [Online]. Available: http://www.bitdefender.es/news/como-trabaja-la-tecnolog%C3%ADa-antivirus-de-bitdefender-389.html. [Accessed: 04-Feb-2016].
[45] “Kaspersky Anti-Virus 2016 | Kaspersky Lab América Latina | Kaspersky Lab América Latina.” [Online]. Available: http://latam.kaspersky.com/productos/productos-para-el-hogar/anti-virus. [Accessed: 04-Mar-2016].
[46] “ESET Nod32 Antivirus - EcuRed.” [Online]. Available: http://www.ecured.cu/ESET_Nod32_Antivirus. [Accessed: 01-Feb-2016].
[47] “Software antivirus, análisis de protección antivirus, Antivirus Plus | McAfee.” [Online]. Available: http://home.mcafee.com/store/packagedetail.aspx?pkgid=276&culture=es-MX. [Accessed: 04-Feb -2016].
[48] “Los algoritmos avanzados posibilitan una nueva generación de antivirus.” [Online]. Available: http://www.tendencias21.net/Los-algoritmos-avanzados-posibilitan-una-nueva-generacion-de-antivirus_a7880.html. [Accessed: 2-Feb-2016].
[49] “AV-Comparatives Independent Tests of Anti-Virus Software - AV-Comparatives.” [Online]. Available: http://www.av-comparatives.org/. [Accessed: 04-Mar-2016].
[50] “VULNERAVILIDAD, TIPOS DE ATAQUES Y FORMAS DE MITIGARLOS EN LAS CAPAS DEL MODELO OSI EN LAS REDES DE DATOS DE LAS ORGANIZACIONES,” *2012*. [Online]. Available: http://repositorio.utp.edu.co/dspace/bitstream/11059/2734/1/0058R173.pdf. [Accessed: 05-Feb-2016].
[51] ISSAF, “Balwant Rathore, Open Sistemas de Información del Grupo de Seguridad (www.oissg.org).” 2010.
[52] “Configurar una clave de seguridad para una red inalámbrica - Ayuda de Windows.” [Online]. Available: http://windows.microsoft.com/es-co/windows/set-security-key-wireless-network#1TC=windows-7. [Accessed: 02-Mar-2016].
[53] “3.3.1.1 Ataque de suplantación de identidad de switch.” [Online]. Available: http://ecovi.uagro.mx/ccna2/course/module3/3.3.1.1/3.3.1.1.html. [Accessed: 02-Mar-2016].
[54] “Guia_comprador_firewalls_2011.pdf,” *2011*. [Online]. Available: http://www.xnetworks.es/contents/PaloAltoNetworks/Guia_comprador_firewalls_2011.pdf. [Accessed: 02-Mar-2016].

Anexo A - Reporte Técnico Generado Por El Software Owasp-Zap

A2 Reporte UDES

Reporte de Alertas de Seguridad de la Aplicación

Nombre del Cliente

SQL Injection - Oracle - Time Based

Descripción

Falla por Inyección SQL puede ser posible

Riesgo

High

Confiabilidad

Medium

URLs vulnerables

1-http://portalcucuta2.udes.edu.co/index.php?option=com_users&view=reset
Parámetros: view
Atacar: field: [view], value [reset' / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / ']
Otra información: El tiempo de consulta es controlable a través del valor del parámetro [reset' / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / '], el cual causó que la solicitud tomara [12.152] milisegundos, mientras que la consulta original, no modificada, tomó [reset] [3.263] milisegundos

Recomendación

No confíe en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación.
En general, comprobar todos los datos de entrado en el servidor.
Si la aplicación usa JDBC, usar PreparedStatement o CallableStatement, con parámetros pasados por '?'
Si la aplicación utiliza ASP, utilice Command Objects ADO con un fuerte tipo de verificación y consultas parametrizadas.
Si la Base de Datos puede usar Stored Procedures (Procedimientos Almacenados), úselos.
¡NO concatenar cadenas en los query (consultas) en el procedimientos almacenados, o utilizar 'exec', 'exec immediate', o su funcionalidad equivalente!
No crear consultas SQL dinámicas usando una sencilla concatenación de cadenas.
Aplique aun lista blanca (whitelist) de caracteres permitidos, o una lista negra (blacklist) de caracteres no permitidos en la entrada (input) del usuario.
Aplique el privilegio mínimo posible al usuario de la base de datos de los privilegios usados.
En particular evitar el uso de los usuarios de base de datos 'sa' o 'db-owner'. Esto no elimina la inyección SQL, pero minimiza su impacto.
Conceder el mínimo acceso de base de datos que es necesario para la aplicación.

SQL Injection - Hypersonic SQL - Time Based

Descripción

Falla por Inyección SQL puede ser posible

Riesgo

High

Confiabilidad

Medium

URLs vulnerables

1-http://portalcucuta2.udes.edu.co/index.php?option=com_users&view=reset
Parámetros: view
Atacar: field: [view], value ['; select "java.lang.Thread.sleep"(5000) from INFORMATION_SCHEMA.SYSTEM_COLUMNS where TABLE_NAME = 'SYSTEM_COLUMNS' and COLUMN_NAME = 'TABLE_NAME' --]
Otra información: El tiempo de consulta es controlable a través del valor del parámetro ['; select "java.lang.Thread.sleep"(5000) from INFORMATION_SCHEMA.SYSTEM_COLUMNS where TABLE_NAME = 'SYSTEM_COLUMNS' and COLUMN_NAME = 'TABLE_NAME' --], el cual causó que la solicitud tomara [20.014] milisegundos, mientras que la consulta original, no modificada, tomó [reset] [4.195] milisegundos

Recomendación

No confíe en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación.
En general, comprobar todos los datos de entrado en el servidor.
Si la aplicación usa JDBC, usar PreparedStatement o CallableStatement, con parámetros pasados por '?'
Si la aplicación utiliza ASP, utilice Command Objects ADO con un fuerte tipo de verificación y consultas parametrizadas.
Si la Base de Datos puede usar Stored Procedures (Procedimientos Almacenados), úselos.
¡NO concatenar cadenas en los query (consultas) en el procedimientos almacenados, o utilizar 'exec', 'exec immediate', o su funcionalidad equivalente!
No crear consultas SQL dinámicas usando una sencilla concatenación de cadenas.
Aplique aun lista blanca (whitelist) de caracteres permitidos, o una lista negra (blacklist) de caracteres no permitidos en la entrada (input) del usuario.
Aplique el privilegio mínimo posible al usuario de la base de datos de los privilegios usados.
En particular evitar el uso de los usuarios de base de datos 'sa' o 'db-owner'. Esto no elimina la inyección SQL, pero minimiza su impacto.
Conceder el mínimo acceso de base de datos que es necesario para la aplicación.

Referencias

Inyección Remota de Comandos OS

Descripción

Técnica de ataque usada para la ejecución no autorizada de comandos del sistema operativo. Este ataque es posible cuando una aplicación acepta la entrada que no es de confianza para construir comandos del sistema operativo de una manera insegura involucrando desinfección inadecuada de datos, y/o llamada inadecuada de programas externos.

Riesgo

High

Confiabilidad

Medium

URLs vulnerables

1-http://portalcucuta2.udes.edu.co/index.php?view=reset%26timeout+%2FT+5&option=com_users
Parámetros: view
Atacar: reset&timeout /T 5

Recomendación

If at all possible, use library calls rather than external processes to recreate the desired functionality.

Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software.

OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations.
This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.

For any data that will be used to generate a command to be executed, keep as much of that data out of external control as possible. For example, in web applications, this may require storing the command locally in the session's state instead of sending it out to the client in a hidden form field.

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, consider using the ESAPI Encoding control or a similar tool, library, or framework. These will help the programmer encode outputs in a manner less prone to error.

A2 Reporte UIS

Reporte de Alertas de Seguridad de la Aplicación

Nombre del Cliente

SQL Injection - PostgreSQL - Time Based

Descripción

Falla por Inyección SQL puede ser posible

Riesgo

High

Confiabilidad

Medium

URLs vulnerables

1-https://www.uis.edu.co/sondeoVirtual/login.seam?s=11
Parámetros: s
Atacar: field: [s], value ["case when cast(pg_sleep(5) as varchar) > '' then 0 else 1 end --]
Otra información: El tiempo de consulta es controlable a través del valor del parámetro ["case when cast(pg_sleep(5) as varchar) > '' then 0 else 1 end --], el cual causó que la solicitud tomara [7.119] milisegundos, mientras que la consulta original, no modificada, tomó [11] [1.244] milisegundos

2-http://www.uis.edu.co/webUIS/es/rss/noticias.jsp?canal=2160.xml&facultad=ppal
Parámetros: canal
Atacar: field: [canal], value [case when cast(pg_sleep(5) as varchar) > '' then 0 else 1 end]
Otra información: El tiempo de consulta es controlable a través del valor del parámetro [case when cast(pg_sleep(5) as varchar) > '' then 0 else 1 end], el cual causó que la solicitud tomara [6.461] milisegundos, mientras que la consulta original, no modificada, tomó [2160.xml] [1.145] milisegundos

3-http://www.uis.edu.co/webUIS/es/academia/facultades/ciencias/escuelas/biologia/index.jsp?variable=6120
Parámetros: variable
Atacar: field: [variable], value ['case when cast(pg_sleep(5) as varchar) > '' then 0 else 1 end --]
Otra información: El tiempo de consulta es controlable a través del valor del parámetro ['case when cast(pg_sleep(5) as varchar) > '' then 0 else 1 end --], el cual causó que la solicitud tomara [6.713] milisegundos, mientras que la consulta original, no modificada, tomó [6120] [218] milisegundos

Recomendación

No confíe en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación.
En general, comprobar todos los datos de entrado en el servidor.
Si la aplicación usa JDBC, usar PreparedStatement o CallableStatement, con parámetros pasados por '?'
Si la aplicación utiliza ASP, utilice Command Objects ADO con un fuerte tipo de verificación y consultas parametrizadas.
Si la Base de Datos puede usar Stored Procedures (Procedimientos Almacenados), úselos.
¡NO concatenar cadenas en los query (consultas) en el procedimientos almacenados, o utilizar 'exec', 'exec

SQL Injection - Oracle - Time Based

Descripción

Falla por Inyección SQL puede ser posible

Riesgo

High

Confiabilidad

Medium

URLs vulnerables

1-http://www.uis.edu.co/webUIS/es/academia/facultades/ciencias/escuelas/matematicas/index.jsp?variable=6140

Parámetros: variable

Atacar: field: [variable], value [6140" / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / "]

Otra información: El tiempo de consulta es controlable a través del valor del parámetro [6140" / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / "], el cual causó que la solicitud tomara [8.830] milisegundos, mientras que la consulta original, no modificada, tomó [6140] [348] milisegundos

Recomendación

No confíe en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación.

En general, comprobar todos los datos de entrado en el servidor.

Si la aplicación usa JDBC, usar PreparedStatement o CallableStatement, con parámetros pasados por '?'

Si la aplicación utiliza ASP, utilice Command Objects ADO con un fuerte tipo de verificación y consultas parametrizadas.

Si la Base de Datos puede usar Stored Procedures (Procedimientos Almacenados), úselos.

¡NO concatenar cadenas en los query (consultas) en el procedimientos almacenados, o utilizar 'exec', 'exec immediate', o su funcionalidad equivalente!

No crear consultas SQL dinámicas usando una sencilla concatenación de cadenas.

Aplique aun lista blanca (whitelist) de caracteres permitidos, o una lista negra (blacklist) de caracteres no permitidos en la entrada (input) del usuario.

Aplique el privilegio mínimo posible al usuario de la base de datos de los privilegios usados.

En particular evitar el uso de los usuarios de base de datos 'sa' o 'db-owner'. Esto no elimina la inyección SQL, pero minimiza su impacto.

SQL Injection - MySQL

Descripción

Falla por Inyección SQL puede ser posible

Riesgo

High

Confiabilidad

Medium

URLs vulnerables

1-http://www.uis.edu.co/webUIS/es/rss/noticias.jsp?canal=2160.xml&facultad=ppal
Parámetros: canal
Atacar: 2160.xml / sleep(5)
Otra información: El tiempo de consulta es controlable a través del valor del parámetro [2160.xml / sleep(5)], el cual causó que la solicitud tomara [6.736] milisegundos, mientras que la consulta original, no modificada, tomó [2160.xml] [1.530] milisegundos

2-http://www.uis.edu.co/webUIS/es/concursoDocente/index.html
Parámetros: idConsecutivo
Atacar: ' / sleep(5) / '
Otra información: El tiempo de consulta es controlable a través del valor del parámetro [' / sleep(5) / '], el cual causó que la solicitud tomara [7.177] milisegundos, mientras que la consulta original, no modificada, tomó [] [115] milisegundos

Recomendación

No confíe en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación.
En general, comprobar todos los datos de entrado en el servidor.
Si la aplicación usa JDBC, usar PreparedStatement o CallableStatement, con parámetros pasados por '?'
Si la aplicación utiliza ASP, utilice Command Objects ADO con un fuerte tipo de verificación y consultas parametrizadas.
Si la Base de Datos puede usar Stored Procedures (Procedimientos Almacenados), úselos.
¡NO concatenar cadenas en los query (consultas) en el procedimientos almacenados, o utilizar 'exec', 'exec immediate', o su funcionalidad equivalente!
No crear consultas SQL dinámicas usando una sencilla concatenación de cadenas.
Aplique aun lista blanca (whitelist) de caracteres permitidos, o una lista negra (blacklist) de caracteres no permitidos en la entrada (input) del usuario.
Aplique el privilegio mínimo posible al usuario de la base de datos de los privilegios usados.
En particular evitar el uso de los usuarios de base de datos 'sa' o 'db-owner'. Esto no elimina la inyección SQL, pero minimiza su impacto.

A3 Reporte Upa Teleco

Reporte de Alertas de Seguridad de la Aplicación

Nombre del Cliente

X-Frame-Options Header Not Set

Descripción

X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Riesgo

Medium

Confiabilidad

Medium

URLs vulnerables

1-http://www.unipamplona.edu.co/telecomunicaciones/upw_top.htm

2-http://www.unipamplona.edu.co/telecomunicaciones/ico_frontis.ico

3-http://www.unipamplona.edu.co/telecomunicaciones/

4-http://www.unipamplona.edu.co/telecomunicaciones

5-http://www.unipamplona.edu.co/sitemap.xml

6-http://www.unipamplona.edu.co/robots.txt

Recomendación

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

Referencias

http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

Método inseguro de HTTP - TRACE

Descripción

The insecure HTTP method [TRACE] is enabled for this resource, and is exploitable. The TRACK and TRACE methods may be used by an attacker, to gain access to the authorisation token/session cookie of an application user, even if the session cookie is protected using the 'HttpOnly' flag. For the attack to be successful, the application user must typically be using an older web browser, or a web browser which has a Same Origin Policy (SOP) bypass vulnerability.

Riesgo

Medium

Confiabilidad

Medium

URLs vulnerables

1-http://www.unipamplona.edu.co/telecomunicaciones/upw_top.htm
Evidencia: QyNL6L1fQnJeuRWPzkkOUeojQxHpLDF5sfziLRmP
Otra información: A TRACE request was sent for this request, with a custom cookie value [QyNL6L1fQnJeuRWPzkkOUeojQxHpLDF5sfziLRmP]. This cookie value was disclosed in the HTTP response, confirming the vulnerability.

2-http://www.unipamplona.edu.co/telecomunicaciones/upw_top.htm
Evidencia: AgbmzI9Rx8uvyeiOjTLwaBnTmS5qlg3f4RBxRtPA
Otra información: A TRACE request was sent for this request, with a custom cookie value [AgbmzI9Rx8uvyeiOjTLwaBnTmS5qlg3f4RBxRtPA]. This cookie value was disclosed in the HTTP response, confirming the vulnerability.

3-http://www.unipamplona.edu.co/telecomunicaciones/ico_frontis.ico
Evidencia: sWjAsg9re88iJ8fTU1WAPeeh0gbITwrLNEGoGAcm
Otra información: A TRACE request was sent for this request, with a custom cookie value [sWjAsg9re88iJ8fTU1WAPeeh0gbITwrLNEGoGAcm]. This cookie value was disclosed in the HTTP response, confirming the vulnerability.

4-http://www.unipamplona.edu.co/telecomunicaciones/ico_frontis.ico
Evidencia: 9tPufz8WxbeKKcOGjUNfrO3bGaR0V1ZlGRzwjNWK
Otra información: A TRACE request was sent for this request, with a custom cookie value [9tPufz8WxbeKKcOGjUNfrO3bGaR0V1ZlGRzwjNWK]. This cookie value was disclosed in the HTTP response, confirming the vulnerability.

5-http://www.unipamplona.edu.co/telecomunicaciones/
Evidencia: iSwq41Keu0qwGaT25xnlze2cGqmB0kUBKCKMD5Zg

X-Content-Type-Options Header Missing

Descripción

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Riesgo

Low

Confiabilidad

Medium

URLs vulnerables

1-http://www.unipamplona.edu.co/telecomunicaciones/upw_top.htm
Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

2-http://www.unipamplona.edu.co/telecomunicaciones/ico_frontis.ico
Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

3-http://www.unipamplona.edu.co/telecomunicaciones/
Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

4-http://www.unipamplona.edu.co/telecomunicaciones
Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

5-http://www.unipamplona.edu.co/sitemap.xml
Otra información: This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

6-http://www.unipamplona.edu.co/robots.txt

A5. Reporte UFPS

Reporte de Alertas de Seguridad de la Aplicación

Nombre del Cliente

Confidencial

SQL Injection - MySQL

Descripción

Falla por Inyección SQL puede ser posible

Riesgo

High

Confiabilidad

Medium

URLs vulnerables

1-http://www.ufps.edu.co/ufpsnuevo/modulos/contenido/view_meeting_link.php?item=107&link=SMMLV
Parámetros: link
Atacar: SMMLV" and 0 in (select sleep(5)) --
Otra información: El tiempo de consulta es controlable a través del valor del parámetro [SMMLV" and 0 in (select sleep(5)) --], el cual causó que la solicitud tomara [7.301] milisegundos, mientras que la consulta original, no modificada, tomó [SMMLV] [1.449] milisegundos

2-http://www.ufps.edu.co/ufpsnuevo/modulos/contenido/view_contenido_link.php?item=120&link=Presentacion
Parámetros: item
Atacar: 120 / sleep(5)
Otra información: El tiempo de consulta es controlable a través del valor del parámetro [120 / sleep(5)], el cual causó que la solicitud tomara [5.877] milisegundos, mientras que la consulta original, no modificada, tomó [120] [384] milisegundos

3-http://www.ufps.edu.co/ufpsnuevo/modulos/contenido/view_contenido__link.php?item=130&link=Plan Anticorrupcion
Parámetros: item
Atacar: 130 / sleep(5)
Otra información: El tiempo de consulta es controlable a través del valor del parámetro [130 / sleep(5)], el cual causó que la solicitud tomara [7.448] milisegundos, mientras que la consulta original, no modificada, tomó [130] [1.613] milisegundos

4-http://www.ufps.edu.co/ufpsnuevo/modulos/contenido/view_contenido.php?item=100
Parámetros: item
Atacar: 100 and 0 in (select sleep(5)) --
Otra información: El tiempo de consulta es controlable a través del valor del parámetro [100 and 0 in (select sleep(5)) --], el cual causó que la solicitud tomara [11.428] milisegundos, mientras que la consulta original, no modificada, tomó [100] [798] milisegundos

Recomendación

No confíe en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación.
En general, comprobar todos los datos de entrado en el servidor.
Si la aplicación usa JDBC, usar PreparedStatement o CallableStatement, con parámetros pasados por '?'
Si la aplicación utiliza ASP, utilice Command Objects ADO con un fuerte tipo de verificación y consultas parametrizadas.
Si la Base de Datos puede usar Stored Procedures (Procedimientos Almacenados), úselos.
¡NO concatenar cadenas en los query (consultas) en el procedimientos almacenados, o utilizar 'exec', 'exec immediate', o su funcionalidad equivalente!
No crear consultas SQL dinámicas usando una sencilla concatenación de cadenas.
Aplique aun lista blanca (whitelist) de caracteres permitidos, o una lista negra (blacklist) de caracteres no permitidos en la entrada (input) del usuario.
Aplique el privilegio mínimo posible al usuario de la base de datos de los privilegios usados.
En particular evitar el uso de los usuarios de base de datos 'sa' o 'db-owner'. Esto no elimina la inyección SQL, pero minimiza su impacto.
Conceder el mínimo acceso de base de datos que es necesario para la aplicación.

Referencias

https://www.OWASP.org/index.php/Top_10_2010-a1
https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

SQL Injection - Hypersonic SQL - Time Based

Descripción

Falla por Inyección SQL puede ser posible

Riesgo

High

Confiabilidad

Medium

URLs vulnerables

1-http://www.ufps.edu.co/ufps/rectoria/Presentacion.php?item=0
Parámetros: item
Atacar: field: [item], value ["; select "java.lang.Thread.sleep"(5000) from INFORMATION_SCHEMA.SYSTEM_COLUMNS where TABLE_NAME = 'SYSTEM_COLUMNS' and COLUMN_NAME = 'TABLE_NAME' --]
Otra información: El tiempo de consulta es controlable a través del valor del parámetro ["; select "java.lang.Thread.sleep"(5000) from INFORMATION_SCHEMA.SYSTEM_COLUMNS where TABLE_NAME = 'SYSTEM_COLUMNS' and COLUMN_NAME = 'TABLE_NAME' --], el cual causó que la solicitud tomara [6.447] milisegundos, mientras que la consulta original, no modificada, tomó [0] [844] milisegundos

Recomendación

No confíe en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación.
En general, comprobar todos los datos de entrado en el servidor.
Si la aplicación usa JDBC, usar PreparedStatement o CallableStatement, con parámetros pasados por '?'
Si la aplicación utiliza ASP, utilice Command Objects ADO con un fuerte tipo de verificación y consultas parametrizadas.
Si la Base de Datos puede usar Stored Procedures (Procedimientos Almacenados), úselos.
¡NO concatenar cadenas en los query (consultas) en el procedimientos almacenados, o utilizar 'exec', 'exec immediate', o su funcionalidad equivalente!
No crear consultas SQL dinámicas usando una sencilla concatenación de cadenas.
Aplique aun lista blanca (whitelist) de caracteres permitidos, o una lista negra (blacklist) de caracteres no permitidos en la entrada (input) del usuario.
Aplique el privilegio mínimo posible al usuario de la base de datos de los privilegios usados.
En particular evitar el uso de los usuarios de base de datos 'sa' o 'db-owner'. Esto no elimina la inyección SQL, pero minimiza su impacto.
Conceder el mínimo acceso de base de datos que es necesario para la aplicación.

Referencias

Source Code Disclosure - SVN

Descripción

El código fuente de la página actual se dio a conocer por el servidor web

Riesgo

High

Confiabilidad

Medium

URLs vulnerables

1-http://www.ufps.edu.co/ufpsnuevo/sientelau
Atacar: http://www.ufps.edu.co/ufpsnuevo/.svn/text-base/sientelau.svn-base
Otra información: The source code for [sientelau] was found at
[http://www.ufps.edu.co/ufpsnuevo/.svn/text-base/sientelau.svn-base]

2-http://www.ufps.edu.co/ufpsnuevo/proyectos/meci
Atacar: http://www.ufps.edu.co/ufpsnuevo/proyectos/.svn/text-base/meci.svn-base
Otra información: The source code for [meci] was found at
[http://www.ufps.edu.co/ufpsnuevo/proyectos/.svn/text-base/meci.svn-base]

3-http://www.ufps.edu.co/ufpsnuevo/proyectos
Atacar: http://www.ufps.edu.co/ufpsnuevo/.svn/text-base/proyectos.svn-base
Otra información: The source code for [proyectos] was found at
[http://www.ufps.edu.co/ufpsnuevo/.svn/text-base/proyectos.svn-base]

4-http://www.ufps.edu.co/ufpsnuevo/pcontenido
Atacar: http://www.ufps.edu.co/ufpsnuevo/.svn/text-base/pcontenido.svn-base
Otra información: The source code for [pcontenido] was found at
[http://www.ufps.edu.co/ufpsnuevo/.svn/text-base/pcontenido.svn-base]

5-http://www.ufps.edu.co/ufpsnuevo/modulos/contenido
Atacar: http://www.ufps.edu.co/ufpsnuevo/modulos/.svn/text-base/contenido.svn-base
Otra información: The source code for [contenido] was found at
[http://www.ufps.edu.co/ufpsnuevo/modulos/.svn/text-base/contenido.svn-base]

6-http://www.ufps.edu.co/ufpsnuevo/modulos
Atacar: http://www.ufps.edu.co/ufpsnuevo/.svn/text-base/modulos.svn-base
Otra información: The source code for [modulos] was found at
[http://www.ufps.edu.co/ufpsnuevo/.svn/text-base/modulos.svn-base]

Anexo B - Reporte Técnico Generado Por El Software Openvas

B1 Reporte UPA

Scan Report

February 2, 2016

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "unipamplona". The scan started at Wed Feb 2 00:04:55 2016 UTC and ended at Wed Feb 24 00:26:41 2016 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1

... continued from previous page ...

Paket 1: 432283973

Paket 2: 432285480

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details:TCP timestamps
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: $Revision: 787 $

References
Other:
URL:http://www.ietf.org/rfc/rfc1323.txt

[return to 201.245.175.175]

2.1.2 Log general/tcp

Log (CVSS: 7.8)
NVT: 3com switch2hub

Summary
The remote host is subject to the switch to hub flood attack.

Description : The remote host on the local network seems to be connected through a switch which can be turned into a hub when flooded by different mac addresses. The theory is to send a lot of packets (¿ 1000000) to the port of the switch we are connected to, with random mac addresses. This turns the switch into learning mode, where traffic goes everywhere. An attacker may use this flaw in the remote switch to sniff data going to this host

... continues on next page ...

1 Result Overview

Host	High	Medium	Low	Log	False Positive
201.245.175.175	0	0	1	17	0
Total: 1	0	0	1	17	0

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

This report contains all 18 results selected by the filtering described above. Before filtering there were 28 results.

2 Results per Host

2.1 201.245.175.175

Service (Port)	Threat Level
general/tcp	Low
general/tcp	Log
general/icmp	Log
general/CPE-T	Log
8000/tcp	Log
53/tcp	Log

2.1.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:

...continues on next page ...

... continued from previous page ...

Reference : http://www.securitybugware.org/Other/2041.html

Vulnerability Detection Result
Fake IP address not specified. Skipping this check.

Solution
Lock Mac addresses on each port of the remote switch or buy newer switch.

Vulnerability Detection Method
Details:3com switch2hub
OID:1.3.6.1.4.1.25623.1.0.80103
Version used: $Revision: 2244 $

Log (CVSS: 0.0)
NVT: OS fingerprinting

Summary
This script performs ICMP based OS fingerprinting (as described by Ofir Arkin and Fyodor Yarochkin in Phrack 57). It can be used to determine remote operating system version.

Vulnerability Detection Result
ICMP based OS fingerprint results: (91% confidence)
Linux Kernel

Log Method
Details:OS fingerprinting
OID:1.3.6.1.4.1.25623.1.0.102002
Version used: $Revision: 2397 $

References
Other:
URL:http://www.phrack.org/issues.html?issue=57&id=7#article

Log (CVSS: 0.0)
NVT: arachni (NASL wrapper)

Summary
This plugin uses arachni ruby command line to find web security issues.
See the preferences section for arachni options.
Note that OpenVAS is using limited set of arachni options. Therefore, for more complete web assessment, you should use standalone arachni tool for deeper/customized checks.

Vulnerability Detection Result
Arachni could not be found in your system path.
OpenVAS was unable to execute Arachni and to perform the scan you

... continues on next page ...

1 Result Overview

Host	High	Medium	Low	Log	False Positive
200.93.148.3	0	0	0	29	0
Total: 1	0	0	0	29	0

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

This report contains all 29 results selected by the filtering described above. Before filtering there were 29 results.

2 Results per Host

2.1 200.93.148.3

Host scan start Wed Feb 2 22:52:41 2016 UTC
Host scan end

Service (Port)	Threat Level
general/tcp	Log
general/icmp	Log
80/tcp	Log
53/tcp	Log
443/tcp	Log
25/tcp	Log
21/tcp	Log
143/tcp	Log
110/tcp	Log

2.1.1 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

Summary
This script performs ICMP based OS fingerprinting (as described by Ofir Arkin and Fyodor Yarochkin in Phrack 57). It can be used to determine remote operating system version.

...continues on next page ...

B.2 Reporte UFPS

Scan Report

February 2, 2016

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "UFPS TAREA". The scan started at Wed Feb 2 22:52:36 2016 UTC and ended at . The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

... continued from previous page ...

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Log Method
Details:ICMP Timestamp Detection
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: $Revision: 2169 $

References
CVE: CVE-1999-0524
Other:
URL:http://www.ietf.org/rfc/rfc0792.txt

[return to 200.93.148.3]

2.1.3 Log 80/tcp

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result
The remote web server type is :
Apache
and the 'ServerTokens' directive is ProductOnly
Apache does not permit to hide the server type.

Solution

Log Method
Details:HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: $Revision: 2499 $

... continued from previous page ...

Vulnerability Detection Result
ICMP based OS fingerprint results: (91% confidence)
Linux Kernel

Log Method
Details:OS fingerprinting
OID:1.3.6.1.4.1.25623.1.0.102002
Version used: $Revision: 2397 $

References
Other:
URL:http://www.phrack.org/issues.html?issue=57&id=7#article

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result
Here is the route from 192.168.1.34 to 200.93.148.3:
192.168.1.34
10.7.84.50
10.7.84.49
200.93.148.3

Solution
Block unwanted packets from escaping your network.

Log Method
Details:Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 2377 $

[return to 200.93.148.3]

2.1.2 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

... continues on next page ...

... continued from previous page ...

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Log Method
Details:ICMP Timestamp Detection
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: $Revision: 2169 $

References
CVE: CVE-1999-0524
Other:
URL:http://www.ietf.org/rfc/rfc0792.txt

[return to 200.93.148.3]

2.1.3 Log 80/tcp

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result
The remote web server type is :
Apache
and the 'ServerTokens' directive is ProductOnly
Apache does not permit to hide the server type.

Solution

Log Method
Details:HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: $Revision: 2499 $