Recepción: 17 de enero de 2017

Aceptación: 10 de marzo de 2017

Publicación: 14 de marzo de 2017

VULNERABILIDADES Y AMENAZAS A LOS SERVICIOS WEB DE LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO

VULNERABILITIES AND MENACES TO WEB SERVICES IN INTRANET'S TECHNICAL UNIVERSITY OF BABAHOYO

Geovanny Vega Villacís[1]

Raúl Armando Ramos Morocho[2]

1. Universidad Técnica de Babahoyo. Facultad de Administración, Finanzas e Informática. Babahoyo, Los Ríos (Ecuador). E-mail: pvega@utb.edu.ec

2. Universidad Técnica de Babahoyo. Facultad de Administración, Finanzas e Informática. Babahoyo, Los Ríos (Ecuador). E-mail: rramos@utb.edu.ec

Citación sugerida:

Vega Villacís, G. y Ramos Morocho, R.A. (2017). Vulnerabilidades y amenazas a los servicios web de la intranet de la Universidad Técnica de Babahoyo. *3C Tecnología: glosas de innovación aplicadas a la pyme*, 6(1), 53-66. DOI: <http://dx.doi.org/10.17993/3ctecno.2017.v6n1e21.53-66/>.

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

RESUMEN

Hoy en día el recurso sustancial a proteger, es sin duda la información. El objetivo de la investigación es demostrar las vulnerabilidades y amenazas que presentan los servicios WEB en la intranet de la Universidad Técnica de Babahoyo. Se determinó las debilidades y ataques presentes en la red; a través de, análisis por observación directa con pruebas de tráfico de paquetes y encuestas a usuarios de red. Se concluye en la falta de procedimientos en seguridad informática y errores no controlados por ataques y perpetraciones. Finalizando con el diseño de un Sistema de Detección de Intrusos (NDIS).

ABSTRACT

Today the substantial resource to protect, is certainly THE INFORMATION. The objective of the research is to demonstrate the vulnerabilities and threats presented by WEB services in the intranet of the Technical University of Babahoyo. We determined the weaknesses and attacks present in the network; through direct observation analysis with tests of packet traffic and surveys to network users. It concludes in the lack of procedures in computer security and errors not controlled by attacks and perpetrations. Finishing with the design of an Intrusion Detection System (NDIS).

PALABRAS CLAVE

Seguridad Informática, Amenazas y Ataques de Red, Sistemas de Detección de Intrusos.

KEY WORDS

Computer Security, Network's Menaces and Attacks, Intrusion Detection Systems.

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

1. INTRODUCCIÓN

Hoy en día, teniendo en cuenta el avanzado ritmo de la tecnología, las empresas e instituciones sean públicas o privadas adoptan medidas de protección y seguridad para preservar su bien más preciado, la información, ya que del mismo modo se han hecho presentes los ataques informáticos e infiltraciones no autorizadas de personal ajeno o mal intencionado para cometer acciones ilícitas o sacar ventaja competitiva.

Es así que las empresas invierten sin escatimar recursos en asesorías y capacitaciones, equipos informáticos, personal preparado y entrenado para afrontar dicho reto y mermar cualquier tipo de irrupción a sus sistemas informáticos. Según (Symantec Corporation, 2015) el 55% de las empresas están reclutando personal en áreas de seguridad informática, un 42% han aumentado los presupuestos de prevención en pérdida de datos y el 45% están aumentado los presupuestos en seguridad Web, redes y puntos finales.

No muy ajena a esta realidad, la Universidad Técnica de Babahoyo (UTB) presenta inconvenientes en su infraestructura tanto al interior como hacia la WAN en materia de seguridad informática. Uno de los aspectos objeto de estudio son las vulnerabilidades y amenazas presentes en la intranet de la institución, orientados a los servicios WEB, siendo necesario evidenciar el uso libre e ilimitado del Internet con acceso a cualquier página web, red social, aplicaciones y sitios de baja confianza, factores que toleran un fácil ingreso e infiltración de personas no autorizadas al interior de la red.

El presente caso de estudio se enfoca en aspectos de seguridad LOGICA y ACTIVA para la intranet de la universidad, permitiendo evidenciar las falencias en materia de seguridad informática y poner a prueba dichas vulnerabilidades con testeos simples de infiltración a puertos sobre los servicios WEB no controlados de la red TCP/IP, y recomendar un plan de mejora a través del diseño elemental de un Sistema de Detección de Intrusos (NDIS).

2. LA SEGURIDAD INFORMÁTICA

La seguridad informática en la actualidad ya no es una ventaja competitiva entre una empresa y otra, es una necesidad, ya que el avance tecnológico ha permitido también el aumento de la delincuencia informática produciendo perjuicios en las organizaciones por pérdida o mala manipulación de la información.

> Según (Symantec Corporation, 2015) *"el 95% de empresas sufrió pérdidas debido a ciberataques incluyendo tiempo de inactividad, robo de identidad de clientes y empleados y robo de propiedad intelectual; el 86% de estas pérdidas se traduce en costos reales. Y el 20% de los negocios perdió por lo menos USD $181,220 como resultado de ciberataques."*

Para evitar y en el mejor escenario minimizar los ataques e infiltraciones no deseadas, es indispensable implementar medidas de protección y seguridad a la infraestructura tecnológica. Adoptar políticas de seguridad informática y diseñar una intranet segura. Solo

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

es posible, a través de un análisis detallado de los distintos protocolos de seguridad, herramientas tecnológicas y aplicaciones informáticas.

La Universidad Técnica de Babahoyo cuenta con una intranet poco segura, provocando poner en alto riesgo las actividades y procesos informáticos de la institución. Es evidente apreciar la facilidad de acceso para cualquier usuario a la red, poder conectarse al internet y acceder en forma libre e ilimitada a cualquier sitio WEB. Por otro lado, las redes sociales están constantemente disponibles y no existe restricción alguna para ejecutar aplicaciones que puedan conectarse fuera de la red.

Parte del gran problema de accesibilidad y control en la red de la institución radica en la falta de gestión y monitoreo a los diferentes puertos y servicios de la red; ya que no cuenta con una red segura efectiva y protegida contra amenazas y ataques perpetrados al interior como hacia afuera, perjudicando casi en un 80% su infraestructura tecnológica para cualquier incidente.

Los equipos de comunicación se encuentran sobredimensionados y mal configurados, y específicamente el equipo proxy (SOPHOS SG330) no actúa efectivamente sobre la seguridad y protección controlando los puertos de entrada y salida de la intranet.

El propósito del presente Caso de Estudio está orientado a:

Demostrar las vulnerabilidades y amenazas que presentan los servicios WEB en la intranet de la Universidad Técnica de Babahoyo, como factor endeble en materia de seguridad informática.

Las preguntas de reflexión para determinar los problemas de investigación son:

- ¿Cuáles son las medidas de seguridad informática implementadas en la intranet de la UTB para un correcto uso del Internet?
- ¿Qué estados de seguridad presentan los puertos TCP/IP con análisis de tráfico de paquetes usando servicios WEB?

La investigación se desarrolla en el perímetro que conforma la Universidad Técnica de Babahoyo, misma que se encuentra situada en el cantón Babahoyo dentro de la zona urbana. Al ser una entidad del estado ecuatoriano, está sujeta a varias obligaciones y regulaciones, entre una de ellas dicta lo siguiente:

Ley Orgánica de Telecomunicaciones. - Artículo 61. Competencias del Órgano Rector - Corresponde a la Institución de Educación Superior:

> 9. Formular las políticas y planes para la creación, regulación y supervisión de la central de datos de la institución, intercambio de información por medios electrónicos, seguridad en materia de información e informática, así como evaluación de su ejecución. (ARCOTEL, 2015)

Seguridad Lógica. - La seguridad lógica complementa a la seguridad física, protegiendo el software y los equipos informáticas. Es decir, las aplicaciones y datos de usuarios de robos, pérdida de datos, modificaciones no autorizadas, etc. A continuación, se enumera las principales amenazas y mecanismos para defenderse (Seoane, César & et al., 2013):

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

Tabla 1. Amenazas y mecanismos de defensa en seguridad Lógica.

AMENAZAS	MECANISMOS DE DEFENSA
ROBOS	• Cifrar la información almacenada en los soportes para que en caso de robo no sea legible. • Utilizar contraseñas para evitar el acceso a lo información. • Sistemas biométricos (uso de huella dactilar, tarjetas identificadoras, caligrafío).
PÉRDIDA DE INFORMACIÓN	• Realizar copias de seguridad para poder restaurar la información perdida. • Uso de sistemas tolerantes a fallos, elección del sistema de ficheros del sistema operativo adecuado. • Uso de conjunto de discos redundantes, protege contra la pérdida de datos y proporciona la recuperación de los datos en tiempo real.
PÉRDIDA DE INTEGRIDAD EN LA INFORMACIÓN	• Uso de programas de chequeo del equipo, SiSoft Sandra 2000, TuneUp, etc. • Mediante la firma digital en el envío de información a través de mensajes enviados por la red. • Uso de la instrucción del sistema operativo Windows, sfc (system file checker).
ENTRADA DE VIRUS	Uso de antivirus, que evite que se infecten los equipos con programas malintencionados.
ATAQUES DESDE LA RED	• Firewall, autorizando y auditando las conexiones permitidas. • Programas de monitorización • Servidores Proxys, autorizando y auditando las conexiones permitidas.
MODIFICACIONES NO AUTORIZADAS	• Uso de contraseñas que no permitan el acceso a la información. • Uso de listas de control de acceso. • Cifrar documentos.

Fuente: Seoane, César; et al. 2013.

Seguridad Activa. - La seguridad activa la podemos definir como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos. A continuación, se enumeran las principales técnicas de seguridad activa (Seoane, César & et al., 2013):

Tabla 2. Técnicas de seguridad activa.

TÉCNICA	¿QUÉ PREVIENE?
USO DE CONTRASEÑAS	Previene el acceso a recursos por parte de personas no autorizadas.
LISTAS CONTROL DE ACCESO	Previene el acceso a los Ficheros por parte de personal no autorizado.
ENCRIPTACIÓN	Evita que personas sin autorización puedan interpretar la información.
USO DE SOFTWARE DE SEGURIDAD INFORMÁTICA	Previene de virus informáticos y de entradas indeseadas al sistema informático.
FIRMAS Y CERTIFICADOS DIGITALES	Permite comprobar la procedencia, autenticidad e integridad de los mensajes
SISTEMAS DE FICHEROS CON TOLERANCIA A FALLOS	Previene fallos de integridad en caso de apagones de sincronización o comunicación
CUOTAS DE DISCO	Previene que ciertos usuarios hagan un uso indebido de la capacidad de disco

Fuente: Seoane, César; et al. 2013.

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

2.1. ELEMENTOS QUE ATENTAN LA SEGURIDAD INFORMÁTICA

Entre los elementos que atentan contra la seguridad de las redes de cómputo encontramos las amenazas físicas y lógicas, catástrofes naturales, acciones humanas, entre otras. Un informe de seguridad de Cisco revela que el 77% de los trabajadores desconoce las principales amenazas de seguridad, poniendo en peligro los datos de sus compañías. El empleado resulta ser el eslabón más débil de la cadena por falta de conciencia y desconocimiento (Casas, 2014).

Por otro lado, durante el desarrollo de aplicaciones los programadores suelen dejar puertas abiertas originadas en ocasiones por errores de programación. Si dicha vulnerabilidad se descubriera o filtrara por cualquier intruso, éste puede hacer uso de ella para violar la integridad del sistema. Empresas de seguridad a nivel mundial reportan que los ataques a datos confidenciales mediante el uso de puertas abiertas durante el primer semestre del 2014, aumentó en un 113% (Symantec Corporation, 2015).

2.2. AMENAZAS LÓGICAS

Las amenazas lógicas son todos los programas que de una forma u otra pueden dañar el sistema informático. Se les conoce con el nombre de *malware*, *bugs* o agujeros. Son errores de programación software que pueden comprometer el sistema operativo. A estos errores se les conoce como *bugs* y los programas que aprovechan de estas vulnerabilidades, *exploits*. Estos últimos son muy peligrosos ya que no se necesita de mucho conocimiento para utilizarlos y comprometer un servidor (Ludwin, 2006).

Las bombas lógicas son partes de código de algún programa que permanecen pasivas hasta que son activadas en un determinado momento y ejecutan su tarea destructiva, y los detonadores suelen ser presencia o ausencia de un fichero específico, una fecha concreta, una combinación de teclas, y otras variantes (Ludwin, 2006). Los VIRUS son también secuencias de códigos que se insertan en un fichero ejecutable denominado huésped, de manera que cuando se active el fichero el virus también lo hará, insertándose a sí mismo en otros programas para asegurar su procreación y diseminación. A estos se le unen los caballos de troya, los cuales son instrucciones escondidas en programas de manera que este parezca realizar las tareas que el usuario espera de él, pero en realidad ejecuta funciones ocultas que atentan contra la seguridad. Los caballos de Troya ocultan su intención real bajo la apariencia de un programa inofensivo (Villalón, 2002).

Ataques por envenenamiento IP O ARP (SPOOFING), las relaciones de confianza basadas en direcciones IP pueden ser burladas por *spoofing*, mediante el cual se suplantada la identidad de la máquina en la que se confía. El *spoofing* puede ser IP o ARP cuando el envenenamiento es ARP es más difícil de detectar porque la máquina del intruso funciona de puente entre las estaciones y no se interrumpe la comunicación (Villalón, 2002). El escaneo de puertos funciona a partir de las respuestas de los protocolos (TCP o UDP) como resultado a los intentos de conexión en determinados puertos, pudiendo obtener información acerca de los servicios ofrecidos por los sistemas operativos y las aplicaciones. Una vez conocida la versión de la aplicación, se consigue sus vulnerabilidades. Casi la totalidad de los sistemas de detección de intrusos son capaces de detectar los escaneos de puertos, el cual no llega a ser un ataque, pero es sin duda la antesala. Como Sistema de Detección de Intrusos basado en Red (NIDS) se recomienda el SNORT, en su versión para Linux. (Villalón, 2002).

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

3. METODOLOGÍA

Para el presente trabajo las metodologías de investigación que más se articulan son la descriptiva y de campo. Definiendo la problemática que presenta la Universidad Técnica de Babahoyo, en: ¿Qué tipos de vulnerabilidades y amenazas presentan los servicios WEB a la intranet de la Universidad Técnica de Babahoyo en materia de seguridad informática?

Estas metodologías permitirán recolectar información y evidenciar los problemas que presenta la Universidad en materia de seguridad informática, identificando sus vulnerabilidades y amenazas perpetradas a la intranet, emplear las técnicas y herramientas necesarias para comprobar el acceso y conectividad que ejecutan los usuarios de la red, y, adicionalmente, dirigir las guías de observación para el testeo de los puertos TCP/IP.

Para la recolección de la información, los instrumentos más adecuados para llevar a cabo la investigación son: Las encuestas y fichas de observación de campo, los mismos que fueron realizados al personal que trabaja en la Universidad. Para llevar a cabo dichos instrumentos fue necesario calcular la muestra simple de la población total de usuarios en la red matriz de la UTB, según se detalla en la siguiente tabla:

Tabla 3. Cuadro distribución de la población (universo).

Nro.	Descripción	Lugar	Población
1	Usuarios de Red	Campus matriz UTB	406
2	Administradores y Operadores red	Dirección de Sistemas, DataCenter de las facultades	10
3	Autoridades inmediatas	Edif. Administrativo y facultades	4
		TOTAL	**420**

Fuente: elaboración propia.

La fórmula estadística para el tamaño de la muestra es la aleatoria simple no estratificada, que al emplear permite calcular el tamaño de la muestra simple del universo. Para calcular el tamaño de la muestra suele utilizarse la siguiente fórmula:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

Hallando el valor de n:

$$n = \frac{420(0{,}5)^2(1{,}96)^2}{(420-1)(0{,}07)^2 + (0{,}5)^2(1{,}96)^2}$$

n = 104 usuarios de red

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

4. RESULTADOS

Seguidamente, se procede a realizar 104 encuestas en forma aleatoria a docentes y empleados de la Universidad de distintas unidades y facultades, obteniendo en resumen los siguientes resultados:

1) ¿Usted como usuario de la red universitaria, trabaja en base a normas y reglamentos en políticas de seguridad informática?

Tabla 4. Respuestas pregunta n. 1.

Indicador	Valor	Porcentaje
Sí	0	0%
No	100	100%

Fuente: elaboración propia.

Gráfico 1. Respuestas pregunta n. 1.
Elaborado por: elaboración propia.

Para la pregunta n. 1 el total de encuestados (usuarios de red) que representa el 100%, afirman no seguir una política de seguridad, ya que la misma no existe.

2) ¿Su equipo informático ha tenido ataques de virus?

Tabla 5. Respuestas pregunta n. 2.

Indicador	Valor	Porcentaje
Siempre	19	19%
Casi siempre	43	43%
Rara vez	32	32%
Nunca	6	6%

Fuente: elaboración propia.

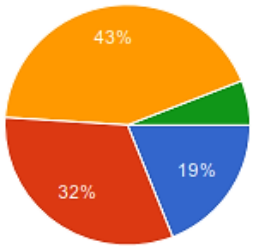

Gráfico 2. Respuestas pregunta n. 2.
Elaborado por: elaboración propia.

En la pregunta n. 2, un 43% de usuarios casi siempre tienen ataques de virus, un 32% rara vez y el 19% de usuarios siempre padecen de ataques de virus. Teniendo apenas un 6% nunca han sufrido de ataques siendo la minoría. En consecuencia, tenemos ataques frecuentes de virus y malwares en la red e internet.

3) ¿Cuándo hace uso del internet con qué frecuencia se le aparecen ventanas emergentes en el navegador que afectan a su equipo?

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

Tabla 6. Respuestas pregunta n. 3.

Indicador	Valor	Porcentaje
Siempre	17	17,3%
Casi siempre	71	72,4%
Rara vez	10	10,3%
Nunca	0	0%

Fuente: elaboración propia.

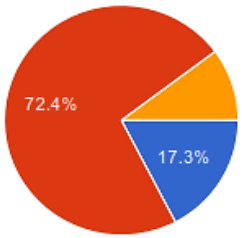

Gráfico 3. Respuestas pregunta n. 3.
Elaborado por: elaboración propia.

En la pregunta n. 3, un 72,4% indican que casi siempre hay presencia de ventanas emergentes, el 17,3% se manifiesta que siempre, y un 10,3% rara vez. En consecuencia, solo pocos usuarios expresan estar conformes con el servicio y la manera de prevenir la presencia de Windows Pop-up´s.

4) ¿Existe un software especial que gestione la seguridad informática de la red, equipos, sistemas y aplicaciones?

Tabla 7. Respuestas pregunta n. 4.

Indicador	Valor	Porcentaje
Sí	5	50%
No	5	50%

Fuente: elaboración propia.

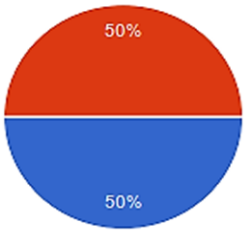

Gráfico 4. Respuestas pregunta n. 4.
Elaborado por: elaboración propia.

En la pregunta n. 4, la mitad de administradores y operadores de red (50%) emplea algún tipo software que gestione la seguridad y protección de la red; mientras que el otro 50% no lo emplea o desconocen.

5) ¿Cuentan con alguna aplicación que monitoree la cantidad de perpetraciones, ataques mal intencionados y errores en la red?

Tabla 8. Respuestas pregunta n. 5.

Indicador	Valor	Porcentaje
Sí	5	55.6%
No	4	44.4%

Fuente: elaboración propia.

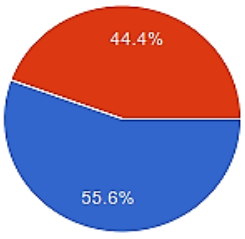

Gráfico 5. Respuestas pregunta n. 5.
Elaborado por: elaboración propia.

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

Para la pregunta n. 5, un 55,6% manifiesta que si tienen una aplicación para monitorear y controlar la red en criterios de seguridad, ataques y perpetraciones, mientras que el otro 44,4% no lo tiene configurado. Por tal razón, se deduce que la red no está totalmente monitoreada y supervisada, dejando todo este ejercicio al departamento de informática de la institución.

4.1. ANÁLISIS DEL TRÁFICO DE PAQUETES PARA COMPROBAR LAS AMENAZAS PRESENTES EN LA INTRANET DE LA UTB

Para proceder con la comprobación de las vulnerabilidades y amenazas que sufre la intranet de la Universidad, se ejecuta el formulario de observación de campo y pruebas in situ. Comenzando por identificar la puerta de enlace que permite la Entrada/Salida de paquetes a la intranet universitaria, para ello se ubica la dirección privada y pública del *gateway* que permite tal tarea siendo en el caso de la UTB, el firewall SOPHOS SG330. Esto se procede realizando una simple consulta de traza y se logra establecer que la IP privada está en el segmento 192.168.0.0/28, mientras que la IP pública asignada es: 181.198.25.129/26.

4.1.1. Análisis de seguridad con inyección de paquetes y puertos no controlados

Para llevar a efecto la ficha de observación y responder las preguntas se ejecutaron programas testeadores de red e inyectores de paquetes para analizar los tipos, tamaños y calidad de los paquetes. Se emplearon los siguientes programas:

a) ZenMap GUI: Es una herramienta gráfica muy amigable que se puede instalar tanto en Linux como en Windows muy fácilmente, ofrece una serie de opciones ya pre configuradas de escaneo, sobre el que únicamente se selecciona el *target* sobre el que se lanzará el escaneo (Corletti E., 2011).

Para esta actividad se utilizará el escaneo de topología y puertos para identificar los puertos de red hábiles y controlados (ver gráfico 7).

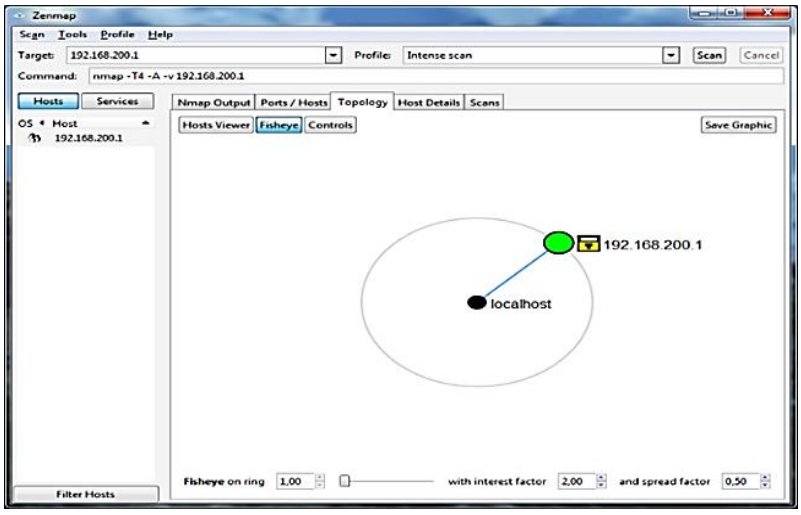

Gráfico 7. Testeo al Firewall SOPHOS. ZenMap 6.4.
Elaborado por: elaboración propia.

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

b) Nemesis 1.4.: Es una herramienta de línea de comandos utilizada para crear aplicaciones personalizadas de IP. Paquetes similares a hping. Puede ser utilizado para crear paquetes TCP y UDP también, pero también ARP, DNS, ETHERNET, ICMP, IGMP, IP, OSPF y RIP también; ósea permite inyectar gran cantidad de paquetes a una red determinada (Andy Wood, 2013).

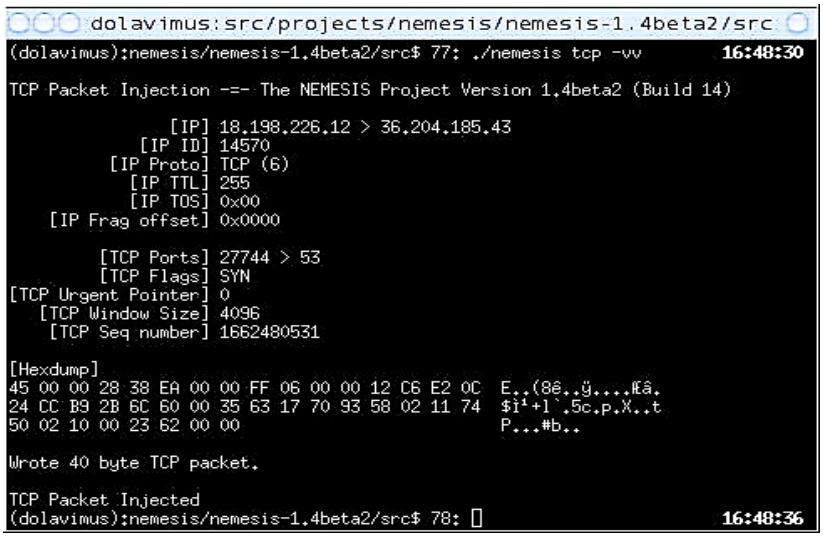

Gráfico 8. Inyección de Paquetes con Nemesis 1,4.
Elaborado por: elaboración propia.

c) SmartSniff: Es una herramienta de análisis de redes / dignostic que le permite capturar paquetes TCP / IP que pasan a través de su adaptador de red. Puede ver los datos capturados como secuencia de conversaciones entre clientes y servidores en modo ASCII (para protocolos basados en texto, como HTTP, SMTP, POP3 y FTP) o como volcado hexadecimal (para protocolos no basados en texto, como DNS) (portablefreeware, 2017).

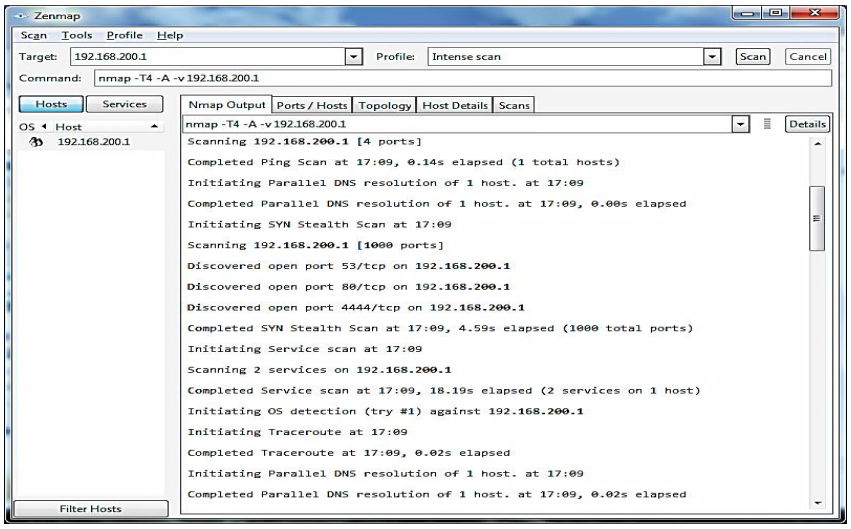

Gráfico 9. Prueba de Ataques y Perpetraciones a la RED-UTB. ZenMap 6.4.
Elaborado por: elaboración propia.

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

El Gráfico 9, visualiza el reporte del análisis de ataques y perpetraciones de paquetes de prueba desde una IP pública 18.198.226.12, usando el programa NEMESIS 1,4. Obteniendo los siguientes resultados (Vega, 2015):

- 36 paquetes peligrosos de 2044 enviados.
- 4 puertos no controlados y cerrados por el firewall SOPHOS.
- No hay control de paquetes por http, no existe aplicaciones.
- No existen puertos seguros controlados para https, ftps, etc.
- No hay resolución de nombres a direcciones IP's privadas establecidas.
- Ausencia de DNS, no existe control de dominio.

4.2. DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS

Para proteger la infraestructura informática de la UTB, se puede acoger al siguiente diseño de Detección de Intrusos a la intranet universitaria.

Para proteger los sistemas informáticos se debe realizar un análisis de las amenazas potenciales, pérdidas que se podrían generar y probabilidad de ocurrencia. A partir de este análisis se diseñan políticas de seguridad que defina reglas y responsabilidades para evitar amenazas y minimizar sus efectos los mismos que se dividen en tres grandes grupos, Prevención, Detección Y Recuperación (Villalón, 2002).

El NIDS (Gráfico 10), debe ser implementado en un punto donde sea capaz de analizar todo el tráfico de la red y equipos que se desea proteger. En la situación de la Universidad caso de estudio, es necesario implementar el equipo servidor NDIS junto al proxy SOPHOS (firewall de la gráfica) de la institución. Tal como detalla la gráfica 10, vendría a ubicarse en la zona verde de protección tanto de entrada como salida de la intranet.

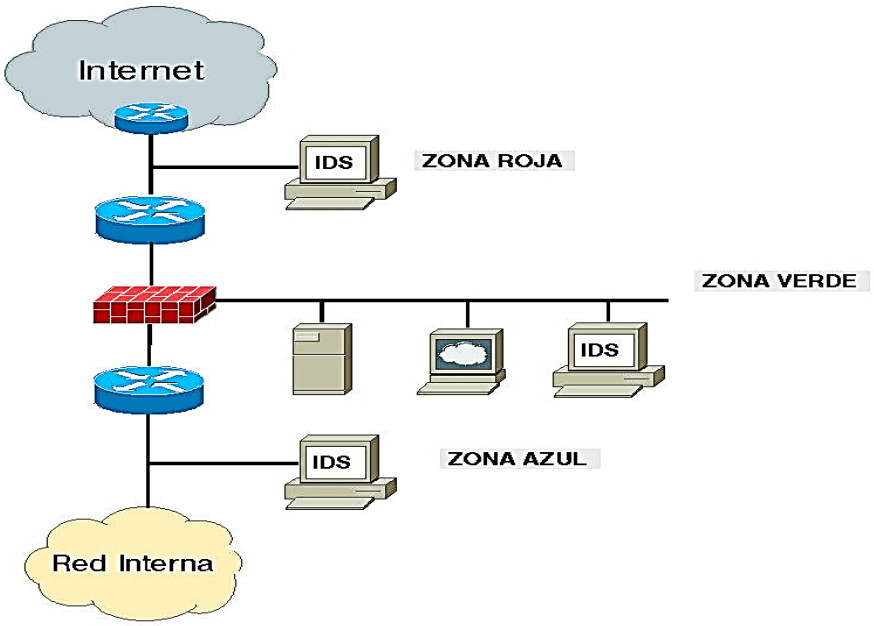

Gráfico 10. Zonas de un IDS dentro de una organización.
Fuente: elaboración propia.

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

5. CONCLUSIONES

- Se determinó que en la intranet de la Universidad Técnica de Babahoyo existen debilidades e incoherencias en las configuraciones de red, ya que no todos los puertos TCP/IP están controlados, no existe un monitoreo detallado de cada una de las subredes y el tráfico de red que hay en cada una de ellas.

- No existe un software específico que gestione las actividades de seguridad informática y gestione eficientemente las conexiones de usuarios de red y monitoree los accesos y usos de internet; provocando que exista libre acceso a sitios no seguros.

- Con la recolección de información de los usuarios y administradores de red, se pudo evidenciar la falta de procedimientos de seguridad en sus equipos informáticos, la carencia de herramientas que ayuden a controlar y supervisar el acceso a los servicios de la intranet, presencia de malwares y ataques constantes de virus, e información basura no deseada para los usuarios.

- No existe una adecuada administración en la infraestructura tecnológica confinando el trabajo al Firewall de Hardware, **SOPHOS** para la interceptación de intrusos y control de accesos; misma que se encuentra parcialmente operativa al estar bloqueada por la falta de licenciamiento y el no poder acceder a él para ser configurado adecuadamente.

- Se recomienda tomar en cuenta las observaciones y tomar las medidas necesarias en materia de seguridad informática, implementar una aplicación NDIS (Sistemas de Red para Detección de Intrusos) y un portal cautivo para acceso de usuarios a los servicios WEB.

3C Tecnología *(Edición 21)* Vol.6 – Nº 1
Marzo – junio'17, 53 – 66
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

5. REFERENCIAS BIBLIOGRÁFICAS

Andy Wood. (Enero de 2013). *ANDY WOOD | Security Professional.* Obtenido de Auditing Firewalls via Packet Crafting with HPing and Nemesis: <https://entsecarch.files.wordpress.com/2014/05/auditing-firewalls-via-packet-crafting-with-nemesis-and-hping-public.pdf/>.

ARCOTEL, A. d. (2015). *Ley Organica de Telecomunicaciones.* Quito: Registro Oficial Suplemento 439.

Casas, A. (30 de octubre de 2014). *Revista Digital CSO Computerworld.* Recuperado el 15 de abril de 2015, de CSO Computerworld: <http://cso.computerworld.es/seguridad-en-cifras/>.

Corletti E., A. (2011). *Seguridad por Niveles.* Madrid: DarFE Learning Consulting .

Ludwin, M. (2006). *The Little Black Book of Computer Virus.* Arizona, American: Eagle publications, Inc.

portablefreeware. (6 de marzo de 2017). *PORTABLEFREEWARE.* Obtenido de SmartSniff v2.27: <https://www.portablefreeware.com/?id=781/>.

Ramos, R. & Gallegos, E. (2016). Infección con ransomware en el servidor de base de datos del sistema Onsystec ERP. 3C Tecnología: glosas de innovación aplicadas a la pyme, 5(4), 56-76. DOI: <http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.56-76/>

Seoane, C. & et al. (2013). *Seguridad informática.* Madrid: McGraw-Hill.

Symantec Corporation. (20 de enero de 2015). *Symantec Internet Security Corporation*. Recuperado el 20 de abril de 2015, de Symantec Internet Security Threat Report: <http://www.symantec.com/security_response/publications/threatreport.jsp/>.

Vega, G. (2015). *Seguridad informática y métodos de protección en infraestructuras tecnológicas y su incidencia en la intranet de la Universidad Técnica de Babahoyo, año 2015". Diseño de una infraestructura tecnológica segura.* Quevedo: UTEQ.

Villalón, A. (2002). *Seguridad en Unix y Redes.* Valencia: Universidad Politécnica de Valencia.