
# ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

## FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

### CARRERA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

# "ANÁLISIS DE VULNERABILIDADES DE SERVIDORES VIRTUALES, CASO PRÁCTICO SERVICIOS WEB INFORMATIVOS DE LA ESPOCH"

**Trabajo de titulación**

Tipo: Propuesta Tecnológica

Presentado para optar al grado académico de:

**INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES**

**AUTOR**: ANGEL SALVADOR ARIAS PAREDES

**DIRECTOR:** ING. MARCO VINICIO RAMOS VALENCIA

Riobamba – Ecuador

2019

Yo, Angel Salvador Arias Paredes, declaro que el presente trabajo de titulación es de mi autoría y los resultados del mismo son autenticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor (a) asumo la responsabilidad legal y academica de los contenidos de este trabajo de titulación. El patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 20 de noviembre de 2019.

**Angel Salvador Arias Paredes**

**060406183-8**

**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**

**FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**

**CARRERA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES**

El tribunal del trabajo de titulación certifica que: El trabajo de titulación: Tipo: Propuesta Tecnológica, **ANÁLISIS DE VULNERABILIDADES DE SERVIDORES VIRTUALES, CASO PRÁCTICO SERVICIOS WEB INFORMATIVOS DE LA ESPOCH,** realizado por el señor/ la señora: **ÁNGEL SALVADOR ARIAS PAREDES,** ha sido minuciosamente revisado por los Miembros del Tribunal del trabajo de titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

| | **FIRMAS** | **FECHA** |
|---|---|---|
| Ing. Mónica Andrea Zabala Haro<br>**PRESIDENTE DEL TRIBUNAL** | _____ | _____ |
| Ing. Marco Vinicio Ramos Valencia<br>**DIRECTOR DEL TRABAJO DE TITULACIÓN** | _____ | _____ |
| Ing. Jonny Israel Guaiña Yungán<br>**MIEMBRO DE TRIBUNAL** | _____ | _____ |

## DEDICATORIA

Dedico el presente trabajo de titulación a Dios por darme la fortaleza de seguir adelante a pesar de las adversidades.

A mis padres que siempre me han apoyado en los momentos difíciles, por su paciencia y apoyo incondicional.

Angel Arias

**AGRADECIMIENTOS**

Agradezco a mis padres por apoyarme en toda mi etapa universitaria, que fueron un apoyo incondicional en todo lo que necesitara teniéndome paciencia y dándome fuerzas para seguir adelante con mis estudios para no desistir.

A mi primo Diego Paredes y su amigo Jaime Ibarra que me ayudaron para guiarme cuando tuve dudas acerca de varios puntos para la realización de mi tesis sin esperar nada a cambio. Al ingeniero Vinicio Ramos y a la ingeniera Ruth Barba que me ayudaron y revisaron de que la realización de la tesis este bien.

***Angel Salvador Arias Paredes***

**TABLA DE CONTENIDO**

ÍNDICE DE TABLAS

**ÍNDICE DE FIGURAS**

**ÍNDICE DE GRÁFICOS**

**ÍNDICE DE ECUACIÓN**

**ÍNDICE DE ANEXOS**

## ÍNDICE DE ABREVIATURAS

| | |
|---|---|
| **DTIC** | Dirección de Tecnologías de la Información y Comunicación |
| **ISSAF** | Information System Security Assesment Framework |
| **NIST** | Instituto Nacional de Estándares y Tecnología |
| **OSSTMM** | Open Source Security Testing Methodology Manual |
| **OWASP** | Open Web Application Security Project |
| **SEGINTE** | Seguridad de la Información y Telemática |
| **XSS** | Secuencia de comandos en sitios cruzados |
| **ZAP** | Zed Attack Proxy |

**RESUMEN**

El presente trabajo de titulación tuvo como objetivo el análisis de vulnerabilidades de los servidores virtuales, caso práctico, los servicios web informativos de la Escuela Superior Politécnica de Chimborazo (ESPOCH). Teniendo como finalidad analizar las vulnerabilidades, se analizó las diferentes metodologías, se realizó una metodología hibrida entre las metodologías analizadas y finalmente se verifico la metodología propuesta en el presente trabajo de titulación. En primer lugar, se realizó la recolección de datos, posteriormente el análisis de vulnerabilidades de los servicios web informativos, con las vulnerabilidades identificadas se procedió a la explotación mediante el ataque de denegación de servicio, posteriormente se implementó una solución que puede ser utiprocediolizada en la ESPOCH y finalmente se realizó los mismos ataques de denegación de servicio para verificar que la solución implementada fuera exitosa comparando el antes y el después de la realización de los ataques con sus respectivos resultados y análisis. En la guía de soluciones propuesta se tiene una secuencia de pasos para realizar el correspondiente análisis de vulnerabilidades que posean los servicios web de la ESPOCH, así como también las vulnerabilidades potenciales que se puede tener en los servicios web según la información que se desee proteger y proponiendo sus posibles soluciones, dependerá de las vulnerabilidades que posean los servicios web, para conocer los tipos de ataques a los que pueden ser más vulnerables y las correspondientes soluciones que se podrán implementar.

**PALABRAS CLAVE:** <SEGURIDAD INFORMÁTICA>, <SERVICIOS WEB>, <SEGURIDAD DE LA INFORMACIÓN>, <ATAQUE DE DENEGACIÓN DE SERVICIO>, <EXPLOTACIÓN DE VULNERABILIDADES>, <METASPLOIT (SOFTWARE)>, <NIST 800 – 144>, <TOP TEN OWASP>.

**ABSTRACT**

The purpose of this degree work was to analyze the vulnerability of virtual servers, practical cases, and the informative web services at Escuela Superior Politecnica de Chimborazo (ESPOCH). Taking the purpose of analyzing the vulnerabilities, the different methodologies were analyzed, a hibrid methodology was carried out among the analyzed methodologies and finalyy, the methodology proposed in this titling work was verified. In the first place, the data collection was carried out, later the vulnerability analysis of the informative web services, with the identified vulnerabilities, the exploitation was carried out through the denial of service attack, later a solution was implemented that can be used in the ESPOCH and finally thesame denial of services attacks were carried out to verify that the solution implemented was successful comparing the before and after the attacks with their respective results and analysis. In the proposed solutions guide there is a sequence of steps to perform the corresponding vulnerability analysis that ESPOCH web services possess, as well as the potential vulnerabilities that it may have in web services according to the information you want to protect and proposing its possible solutions, will dependo n the vulnerabilities that web services possess, to know the types of attacks to which they may be most vulnerable and the corresponding solutions that can be implemented.

**Keywords:** <Computer security>, <Web services>, <Information security>, <Service denedation attack>, <Vulnerability explotation>, <Metasploit (Software)>, <NIST 800 – 144>, <Top ten OWASP>

## INTRODUCCIÓN

Actualmente, la información que manejan y protegen las empresas es de vital importancia, ya que puede contener información delicada de cada uno de sus clientes, por lo cual, las empresas en los últimos años invierten grandes sumas de dinero en la seguridad informática, dependiendo la empresa toma más énfasis en ciertas vulnerabilidades dependiendo de los datos que consideren ellos más importantes.

La seguridad de redes, así como los ataques y vulnerabilidades siempre existirán y por ello es de suma importancia tener bien protegidos los datos. En el cual existen varias vulnerabilidades que pueden ser explotadas mediante, por ejemplo: ataques SQL Inyection, Denegación de servicio, sobrecarga del buffer, entre otras. El ataque que se realiza depende de la información que se protege en los servicios web informativos lo más importante es que el usuario disponga de acceso a la información que desea mostrar la empresa, lo cual va relacionado con la disponibilidad.

El desarrollo del presente trabajo de titulación se tomó en cuenta varias metodologías como son: NIST 800 – 144, ISSAF, OSSTMM y OWASP. Para con el análisis de las cuatro metodologías sacar una híbrida, ya que no existe una metodología puntual para el análisis de los servidores virtuales, más específico los servicios web informativos. Se realizó mediante una simulación en un nodo de la infraestructura de la ESPOCH simulando los tres servicios web informativos más utilizados por los estudiantes y posteriormente proponiendo una mitigación que puede ser implementado por los encargados de la seguridad en el DTIC. El presente trabajo de titulación tiene la finalidad de dar una mejor experiencia a los usuarios finales de la ESPOCH con sus servicios web informativos, dando así mayor seguridad y una mejor experiencia.

**ANTECEDENTES**

En la era de la informática es de suma importancia el manejo óptimo de los recursos informáticos. Se utiliza la virtualización porque permite aprovechar al máximo los recursos, a la par de que se busca permitir que se ejecuten varios sistemas operativos en un solo hardware, y a la vez sacando el mayor provecho a los recursos. En los años 90 se hizo necesario bajar costos administrativos, fue entonces que Intel como AMD lanzaron modelos que puede soportar tecnología virtual. (Jones & González, 2008, p.2).

La virtualización ha ido evolucionando con el paso de los años, comenzando en el año 1998 cuando se funda la empresa VMware, posteriormente VMware lanza su primer producto en el año 1999 el cual es conocido como VMware Workstation. En el año 2003 la familia de gnu Linux lanza el primer sistema de virtualización libre el cual es conocido como XEN. En el año 2005 Intel introduce su tecnología VT-x (Vanderpool) en arquitectura x86. Y en el año 2006 AMD introduce su tecnología AMD-V (Pacifica). En el año 2007 VirtualBox Open Source Edition (OSE) se libera como un software libre. En 2008 Qumranet, la empresa detrás de KVM es comprada por Red Hat, y en el mismo año Innotek, la empresa detrás de Virtual Box, es comprada por Sun Microsystems. VMware decide convertir VMware ESXi en freeware y Microsoft lanza la versión final de Hyper-V. En el año 2010 Virtual Box pasa a llamarse Oracle VM VirtualBox, y finalmente en el año 2011 se empiezan a incluir ciertas partes de XEN en la rama oficial del kernel de Linux 2.6.37. Integración completa en la versión 3.0. (Alacot, 2011, p.5-9)

La virtualización de servidores se sitúa, en la actualidad, en una de las facetas más importantes dentro de la tendencia de modernización e implantación de las nuevas tecnologías en el mundo empresarial. Estos sistemas incluyen la virtualización del almacenaje, red y control de carga de trabajo. La virtualización en los sistemas informáticos se usa para paliar, y en muchos casos eliminar, la infrautilización de servidores, haciendo un uso más eficiente de los recursos del servidor, mejorando su disponibilidad, facilitando la recuperación, y descentralizando los servicios de administración. ( Doña, García, López, Pascual y Pascual, 2010, p.1)

Al observar la falta de seguridad y poco nivel de rendimiento que presentan los equipos de las empresas, se pudo dar la propuesta de realizar una virtualización en los servidores, lo cual permitirá tener una restauración de toda la información con copias de seguridad ante un desastre y mejorar su nivel de rendimiento. (Landi, 2012, p.1) El impacto que se tendrá principalmente con la virtualización será en el ámbito monetario ya que se podrá realizar la implementación de servidores en un mismo terminal; y, utilizando al máximo todos sus recursos. Permitirá un aislamiento de las particularidades de los dispositivos. Se consigue que el usuario pueda visualizar los recursos que necesita como si fueran dedicados. Permite homogeneizar todos los recursos, por lo que se llega a estandarizar procedimientos y configuraciones. Mejorando a la vez la tolerancia a fallos. Además, también la virtualización aporta: mayor eficiencia, flexibilidad y soporte al uso dinámico de procesos, disminución del consumo eléctrico y aumentando la capacidad de respuesta. (Doña, García, López, Pascual y Pascual, 2010, p.3)

Para el análisis de vulnerabilidades de los servidores virtuales no existe concretamente una norma, por lo tanto, se utilizará la National Institute of Standards and Technology (NIST) 800 – 144 como base, la cual se encuentra destinada al análisis de vulnerabilidades para cloud computing, y a la par se utilizarán otras normas que sean necesarias para poder obtener los mejores resultados. (Jansen y Grance, 2011)

En el ámbito internacional, se tiene como referencia una tesis ya realizada en Bucaramanga – Colombia, con el título "Análisis de vulnerabilidades en aplicaciones Web desarrolladas en PHP Version 5.6.24 con base de datos en MySQL Version 5.0.11 a partir de ataques SQL Inyección", en el cual se hace un análisis de vulnerabilidades en una base de datos MySQL mediante la metodología "OWASP Testing Guide de OWASP (Versión 4)", en la cual se utilizó el tipo de ataque SQL Inyección. (Amado, Ayala y Sierra, 2017, p. 1).

En la institución "Pontifica Universidad Católica del Ecuador", se realizó un estudio comparativo de las distribuciones Linux orientados a la seguridad de redes de comunicación, efectuado por el señor David Hernán Badillo Bernal, en donde se obtuvo los resultados de que la mejor distribución de Linux para la seguridad de redes de comunicación es Centos con un puntaje de novecientos ochenta y dos puntos sobre mil, del análisis que se realizó en la "Pontifica Universidad Católica del Ecuador". (Badillo y Chafla, 2015).

En la Escuela Superior Politécnica de Chimborazo existe un trabajo similar el cual es: "Análisis de vulnerabilidades del servidor E-LEARNING de la ESPOCH para la implementación de mejores prácticas de Seguridad – Acceso", el cual consiste en la ejecución de varios ataques para identificar los más efectivos los resultados de cuáles son los ataques más efectivos frente al E-LEARNING de la ESPOCH. (Alvarado y Montesdeoca, 2017).

## FORMULACIÓN DEL PROBLEMA

¿Cómo se determinarán las vulnerabilidades que enfrentan los servidores virtuales?

## SISTEMATIZACIÓN DEL PROBLEMA

¿Cuáles son todas las vulnerabilidades que enfrentan los servidores virtuales?

¿De qué forma se determinarán las mejores metodologías para el análisis de vulnerabilidades de los servidores virtuales?

¿Qué se aportará para el análisis de vulnerabilidades de servidores virtuales?

¿Cómo se evaluará el ambiente y que impacto tienen estas vulnerabilidades en los servidores virtuales?

## JUSTIFICACIÓN TEÓRICA

En el presente proyecto, se va a realizar el análisis de vulnerabilidades de los servicios web informativos de licenciamiento libre que posee la Escuela Superior Politécnica de Chimborazo en un nodo de la infraestructura de la ESPOCH que es muy similar por motivos de políticas de seguridad.

Se va a realizar una simulación para el análisis de vulnerabilidades para los servicios web informativos de licenciamiento libre de la ESPOCH, utilizando sistemas de virtualización libre tales como Oracle VM VirtualBox, para poder determinar las vulnerabilidades que enfrentan los servicios

web informativos de la ESPOCH, a la par de realizar una guía de pasos para poder tener un manual para cuando se necesite realizar un análisis de vulnerabilidades en diferentes servidores virtuales.

En el presente proyecto se van a utilizar varias metodologías ya que no existe una específica para virtualización, se utilizará la National Institute of Standards and Technology (NIST) 800 - 144, como principal ya que se utiliza para cloud computing, Open Web Application Security Project (OWASP) pues son técnicas que se utilizan para probar la seguridad de las aplicaciones web bajo ciertas circunstancias, Information Systems Security Assesment Framework (ISSAF) ya que permite realizar la evaluación de seguridad de una organización permitiendo resaltar las vulnerabilidades del sistema identificado e identificar sus debilidades y la Open Source Security Testing Methodology Manual (OSSTMM) para saber cuáles son los pasos a tener en cuenta para encontrar las vulnerabilidades de los servidores virtuales.

## JUSTIFICACIÓN APLICATIVA

Se utilizará un nodo de la infraestructura de la ESPOCH para la simulación, en la cual, se realizará en el software GNS3, en donde se simulará los servidores virtuales que posee la Escuela Superior Politécnica de Chimborazo, se utilizará equipos Cisco y para los servidores se los montará en el sistema operativo de Centos y la máquina atacante para las pruebas será con sistema operativo de Kali Linux, para el análisis de vulnerabilidades se realizará con la aplicación OWASP ZAP.

Las etapas que se tiene planificado para el desarrollo del presente trabajo de titulación, en primer lugar, se realizará un estudio de los servicios web informativos más utilizados de la Escuela Superior Politécnica de Chimborazo, luego se simulará la red para analizar, así como también los servidores y la máquina virtual atacante, posteriormente se analizarán las vulnerabilidades que enfrentan dichos servicios web informativos. Sabiendo que una de las principales vulnerabilidades de los servicios web informativos se encuentra relacionada a la disponibilidad, se realizará ataques de denegación de servicio. Habiendo realizado los ataques correspondientes se procederá a la implementación de una posible mitigación que puede ser implmentada en la ESPOCH y se realizarán las pruebas nuevamente para verificar que exista una mejora entre el antes y el después.

## OBJETIVOS

### OBJETIVO GENERAL

Analizar las vulnerabilidades de servidores virtuales, caso práctico servicios web informativos ESPOCH.

### OBJETIVOS ESPECÍFICOS

- Analizar las vulnerabilidades que enfrentan los servidores virtuales de licenciamiento libre.
- Determinar las mejores prácticas para el análisis de las vulnerabilidades en servidores virtuales, comparando las metodologías de seguridad existentes como: NIST 800 – 144, OWASP, ISSAF y OSSTMM.
- Proponer una guía para el análisis de vulnerabilidades de servidores virtuales y su respectiva mitigación.
- Evaluar las mejores prácticas en ambiente simulado, explotando las vulnerabilidades de los servicios web informativos de licenciamiento libre que posee la ESPOCH.

# CAPÍTULO I

## 1. MARCO TEÓRICO

### 1.1. Evolución de sistemas de almacenamiento de red

Usando tecnología de computación en la nube, permite a sus proveedores suministrar almacenamiento virtualizado bajo demanda y almacenar cantidades masivas de datos de sus usuarios en redes de centros de datos distribuidos, siento transparentes para el usuario final la localización exacta de su información, que puede estar situada en cualquier lugar del planeta. (Wheleer y Winburn, 2015, citado en Galmés, 2016, p.9).

#### *1.1.1. Virtualización*

Virtualizar ha sido considerado históricamente y de manera general como tomar algo en cierto estado y hacer parecer que se encuentra en otro estado diferente. A partir de ello, dos aproximaciones han ido evolucionando: hacer parecer que un computador se trata de múltiples computadores y no solamente de uno –virtualización- o lograr que múltiples computadores sean uno sólo; esto, más que virtualización, comúnmente es llamado Grid Computing o Server Aggregation. (Villar, López y Montoya, 2010, p.16-17).

#### *1.1.2. Evolución del almacenamiento en la nube*

De acuerdo a Galmés (2016). La evolución en la nube se puede detallar en forma cronológica de la siguiente manera:

- **1956:** IBM desarrolla el primer disco duro con capacidad para 3.75 MB. Aun no existe tecnología de acceso a datos remotos
- **1969:** Nace la red ARPANET, desarrollada por el departamento de defensa en EE.UU. Ya se puede acceder a los datos situados en otro equipo de forma remota.
- **1979:** EMC2 empieza a promocionar la primera nube privada. Los dispositivos de almacenamiento se encuentran dentro de las organizaciones.

- **1982:** IBM desarrolla el adaptador Ethernet, que permite conexiones rápidas y a bajo costo para acceder de forma online al almacenamiento remoto.
- **Década de 1990:** Realización de backups de forma online. Durante el surgimiento de las empresas punto-com, aparecen los primeros servicios de backup online a través de internet.
- **1996:** La armada estadounidense lanza el proyecto Ethernet denominado IT-2, para el desarrollo de una red con el objetivo de compartir información de forma segura.
- **2006:** Surge Amazon AWS S3. Puede decirse que Amazon lanza la computación en la nube tal y como se conoce hoy en día. S3 es su servicio de almacenamiento en la nube que aún continúa ofreciendo.
- **2007:** Aparece la primera reléase de Dropbox y con este el almacenamiento en la nube personal. Aplica un modelo de servicio gratuito, donde los usuarios pueden ocupar cierta cantidad de datos antes de empezar a cobrar por el servicio. Usa el servicio S3 de Amazon para almacenar los datos de sus usuarios.
- **2008:** Se pone a disposición del público de 38 países el producto de almacenamiento en la nube de Microsoft, SkyDrive, precursor de OneDrive.
- **2012:** Google lanza su servicio Google Drive como evolución de Google Docs. En el año 2013 ya tenía unos 120 millones de usuarios.
- **2015:** Existen multitud de proveedores que ofrecen almacenamiento en la nube y millones de usuarios que lo utilizan.

### *1.1.3. Infraestructura de redes*

Entre las arquitecturas más importantes se consideran los siguientes elementos:

- Cliente

El cliente es el proceso que permite al usuario formular los requerimientos y pasarlos al servidor, se le conoce con el término front-end. (Neilla, 2003, citado en Márquez y Zulaica, 2004 p.3)

El Cliente normalmente maneja todas las funciones relacionadas con la manipulación y despliegue de datos, por lo que están desarrollados sobre plataformas que permiten construir interfaces gráficas de usuario (GUI), además de acceder a los servicios distribuidos en cualquier parte de una red. (Neilla, 2003, citado en Márquez y Zulaica, 2004, p.3)

- Servidor

Es el proceso encargado de atender a múltiples clientes que hacen peticiones de algún recurso administrado por él. Al proceso servidor se le conoce con el término back-end. (Neilla, 2003, citado en Márquez y Zulaica, 2004, p.4)

El servidor normalmente maneja todas las funciones relacionadas con la mayoría de las reglas del negocio y los recursos de datos. (Neilla, citado en Márquez y Zulaica, 2004, p.4)

- Cliente – servidor

Desde el punto de vista funcional, se puede definir la computación Cliente/Servidor como una arquitectura distribuida que permite a los usuarios finales obtener acceso a la información en forma transparente aún en entornos multiplataforma. (Carnegi, 2003, citado en Márquez y Zulaica, 2004, p. 1).

En el modelo cliente servidor, el cliente envía un mensaje solicitando un determinado servicio a un servidor (hace una petición), y éste envía uno o varios mensajes con la respuesta (provee el servicio). En la Figura 1-1 se puede observar como es el modelo de la arquitectura de cliente/servidor. (Neilla, 2003, citado en Márquez y Zulaica, 2004, p.2-3)


**Figura 1-1:** Modelo cliente/servidor.

**Fuente:** Márquez B. & Zulaica J.; 2004, p.4.

## 1.2. Máquina virtual e hipervisor

### *1.2.1. Máquina virtual*

Las máquinas virtuales de hardware o de sistema, que son las que conforman el corazón del modelo de virtualización que será aplicado en el desarrollo del proyecto (virtualización de plataforma), son las que corren paralelamente sobre una máquina física anfitrión o host, de manera que tienen acceso y hacen uso de los recursos hardware que son abstraídos de él. Cada máquina virtual es engañada ya que cree que posee de forma exclusiva los recursos hardware de los que dispone cuando en realidad

lo hace de manera virtual, ejecuta una instancia de sistema operativo sobre el que corren determinados servicios o aplicaciones tal y como consideremos necesario (véase la Figura 2-1 en contraposición a la Figura 3-1, que recoge un servidor sin virtualización y por tanto sin máquinas virtuales). (Villar, López y Montoya, 2010, p. 25).

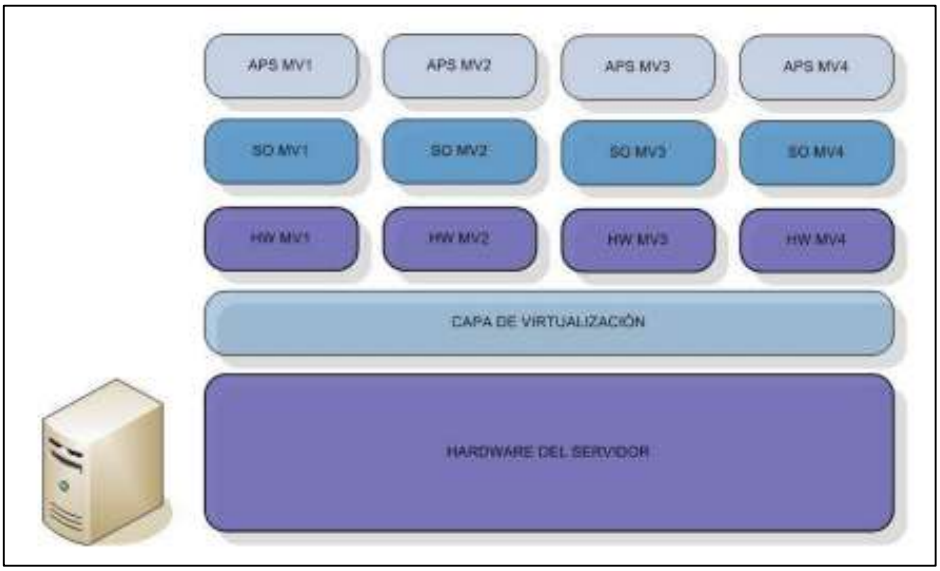



**Figura 2-1:** Arquitectura general de Virtualización sobre un servidor.

**Fuente:** Villar, López y Montoya; 2010, p.25

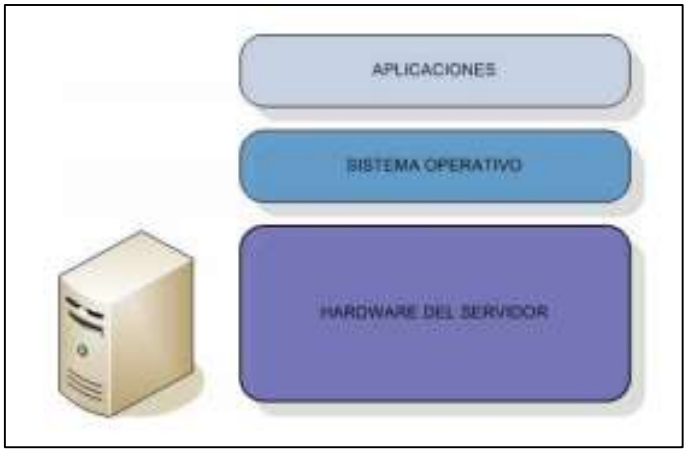



**Figura 3-1:** Arquitectura general de un servidor sin Virtualización.

**Fuente:** Villar, López y Montoya; 2010, p. 26

### *1.2.2. Hipervisor*

El hipervisor o hypervisor es un pequeño monitor de bajo nivel de máquinas virtuales que se inicia durante el arranque, antes que las máquinas virtuales, y que normalmente corre justo sobre el hardware (denominado en alguna bibliografía como native o baremetal) como podemos observar en la Figura 4-1, aunque también lo puede hacer sobre un sistema operativo (llamado en este caso hipervisor hosted). (Villar, López y Montoya, 2010, p.26). Debido a que podemos ejecutar varias máquinas virtuales en un sólo servidor, podemos dejar atrás el modelo "una aplicación por servidor" y consolidar servidores, lo que permite pasar de utilizar el hardware de un servidor en una media de un 10-15% a un 80% como se puede observar en la figura 5-1. (Márquez y Solano, 2011, p.7)

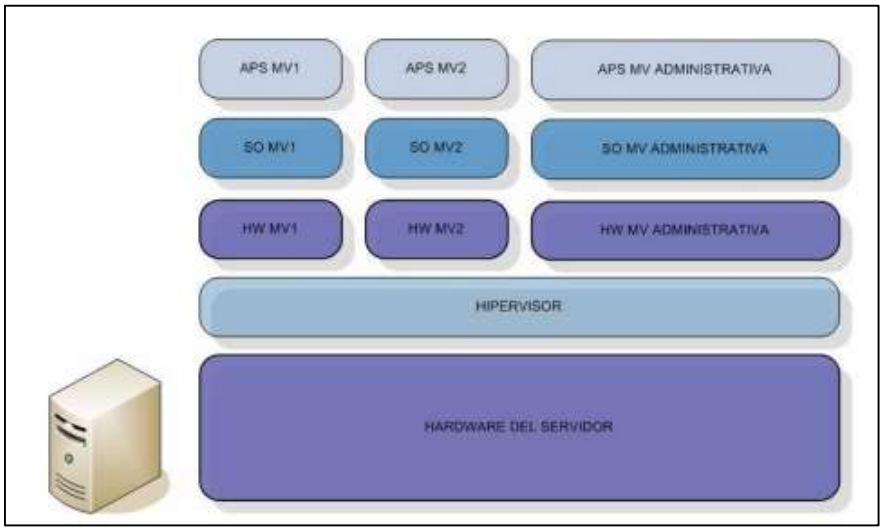



**Figura 4-1:** El hipervisor corre justo sobre el hardware del servidor.

**Fuente:** Villar, López y Montoya; 2010, p.27

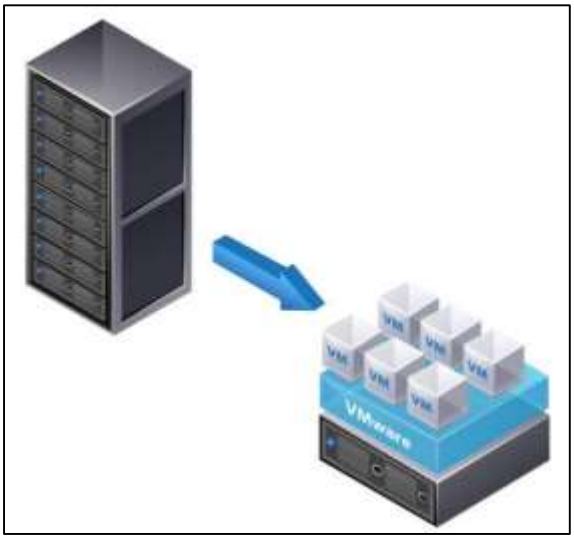


**Figura 5-1:** Virtualización de servidores en hipervisor.
**Fuente:** Márquez y Solano; 2011, p.7

*1.2.2.1. Hipervisor tipo 1*

Este tipo de hipervisores se ejecuta directamente sobre el hardware real, el cual permite controlar este hardware y los sistemas operativos que se encuentran virtualizados. Se dice que los hipervisores tipo 1 son teóricamente más eficientes. Ejemplos de hipervisores tipo 1 se tienen: (Gutiérrez, 2014, p.7)

> El hipervisor bare-metal tiene acceso directo sobre los recursos hardware y no funciona bajo un sistema operativo instalado, una de las ventajas es que se obtendrá un mejor rendimiento, escalabilidad y estabilidad, y una desventaja es que por ser construido con un conjunto de drivers limitados el hardware soportado también es limitado. (vmware esx server, 2013, citado en Tierra y Bonilla, 2014, p.40)

- **VMWare ESXi®:** ofrece una mayor seguridad y fiabilidad ya que supone una menor superficie de ataque con menos código al que aplicar el parche. Una de las ventajas es su simplicidad, ya que se realiza el manejo mediante la utilización de menús. (vmware, 2014, citado en Gutiérrez, 2014, p.8)

- **VMWare ESX®:** se instala directamente en el hardware del servidor proporciona mayor escalabilidad del sector, a comparación de VMWare ESXi® reduce de forma considerable el

espacio que ocupa mediante la eliminación de la consola de servicio, proporciona la tendencia de migrar desde la interfaz local a línea de código. (vmware, 2009, citado en Gutiérrez, 2014, p.8-9).

- **Xen:** permite la ejecución de múltiples sistemas operativos guest con niveles sin precedentes de rendimiento y recursos aislados. Es un software de código abierto. (xen , 2008, citado en Gutiérrez, 2014, p.9)

- **Citrix XenServer®:** es una plataforma de virtualización de código abierto líder en el sector para administrar la infraestructura virtual de nube, servidores y escritorios. (Gutiérrez A., 2014, p.9)

*1.2.2.2. Hipervisor tipo 2*

En este tipo de hipervisor, la aplicación hipervisora o monitor se ejecuta sobre un sistema operativo convencional para luego virtualizar diversos sistemas operativos. Aquí la virtualización se encuentra en una capa más alejada del hardware, y el rendimiento del hipervisor es menor que en los anteriores. Los hipervisores de tipo 2 se encuentran más orientados hacia el usuario final. Los desarrolladores de Xen afirman que KVM es un hipervisor de tipo 2. Ejemplos de hipervisores tipo 2 que se tienen: (Gutiérrez, 2014, p.9)

- **Oracle VM Virtual Box®:** es un producto de virtualización para la empresa AMD64/Intel64, así como también para el uso doméstico. Es un software de código abierto. (VirtualBox, 2014, citado en Gutiérrez, p. 10)

- **Windows Virtual PC®:** es un sistema el cual permite ejecutar más de un sistema operativo a la vez en un equipo, así como también la ejecución de muchas aplicaciones de productividad en entorno virtual de Microsoft Windows®. (Microsoft Windows Virtual PC, 2014, citado en Gutiérrez, p. 10)

- **VMWare Player®:** es un producto gratuito el cual permite ejecutar máquinas virtuales que fueron creadas con productos de VMWare. (Gutiérrez A., 2014, p. 10)

- **VMWare Workstation®:** permite ejecutar múltiples sistemas operativos tanto como Microsoft Windows y GNU/Linux de una manera simultánea e independiente en un solo dispositivo en máquinas virtuales en red que son totalmente portátiles. (vmware, 2014, citado en Gutiérrez, p.10).

En la Figura 6-1 se puede visualizar la diferencia que existe entre el hipervisor tipo 1 con el hipervisor tipo 2, en el cual se puede destacar que el hipervisor tipo 1 en todo el hardware real corre el hipervisor, mientras que en el tipo 2 corre sobre el hardware real el sistema operativo y el software de virtualización utilizando todos los recursos de manera simultánea.

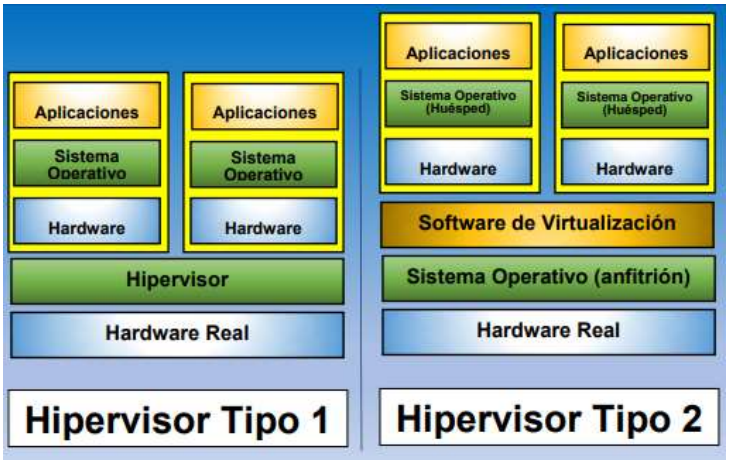



**Figura 6-1:** Tipos de Hipervisores.

**Fuente:** Gutiérrez; 2014, p. 11

*1.2.2.3. Hipervisores híbridos*

Los hipervisores híbridos son la unión de los grupos antes mencionados, aquí tanto el hipervisor, sistema operativo y host van a competir por hardware. En este tipo se menciona a Virtual Server de Microsoft y Virtual Box de Oracle. En la Figura 7-1 se observa cómo funcionan los hipervisores híbridos. (Tierra M. & Bonilla J., 2014, p. 40)

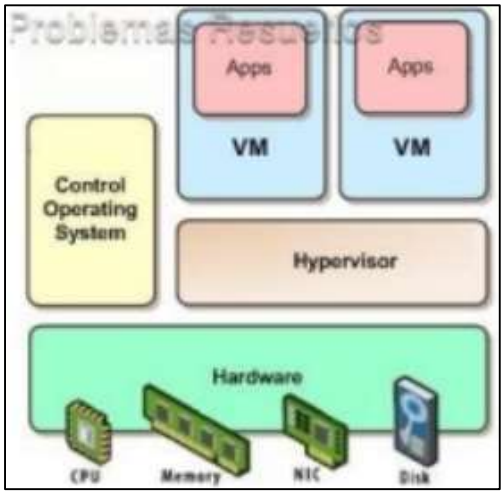



**Figura 7-1:** Hipervisores híbridos.

**Fuente:** Tierra M. y Bonilla J.; 2014, p. 40

En la tabla 1-1 se puede visualizar una clasificación de cada tipo de virtualizador, el tipo de licencia, el tipo de hipervisor tipo 1 o tipo 2 que corresponden y el año en que se publicaron:

**Tabla 1-1:** Descripción general de diferentes tipos de hipervisores.

| Hipervisor | Licencia | Tipo | Año de lanzamiento |
|---|---|---|---|
| **VMWare Workstation** | Proprietary | Tipo 2 | 1999 |
| **VMWare ESXi** | Proprietary | Tipo 1 | 2002 |
| **Xen** | Open Source | Tipo 1 | 2003 |
| **Oracle VirtualBox** | Open Source | Tipo 2 | 2007 |
| **Microsoft Hyper-V** | Proprietary | Tipo 1 | 2008 |
| **XenServer** | Proprietary | Tipo 1 | 2008 |
| **Red Hat Enterprise Virtualization (RHEV)** | Proprietary | Tipo 1 | 2010 |
| **KVM** | Open Source | Tipo 1 y Tipo 2 | 2012 |

**Fuente:** Gkortzis, Rizou y Spinellis, 2016, p. 2

**Realizado** por: Arias, Angel; 2019.

### 1.3. Seguridad de la información

En los últimos años la seguridad de la información ha tomado una relevancia importante en las empresas, ya que es más que un problema de seguridad de datos en las computadoras. En donde se

debe estar orientado a la protección de la propiedad intelectual y la información importante tanto de las empresas como las organizaciones. (Tarazona, 2007, p. 137).

La seguridad informática puede entenderse como aquellas técnicas y/o actividades que se encuentran destinadas a prevenir, proteger y resguardar lo que se considera como susceptible de robo, perdida o daño. (Toapanta, Yanchapaxi y Orestila, 2006, p.8).

Para poder realizar un análisis de la seguridad de la información se toman en cuenta los parámetros principales los cuales son: disponibilidad, integridad y confidencialidad. (Toapanta, Yanchapaxi y Orestila, 2006, p.8).

### *1.3.1. Disponibilidad*

Para poder tener disponibilidad en los servidores virtuales, se puede alcanzar realizando soluciones tanto de software como de hardware. Para las soluciones de software se llega a una alta disponibilidad configurando determinadas herramientas y aplicaciones que han sido diseñadas para tal efecto. Mientras que las soluciones de hardware dependen del tipo de datos o servicios a los que queremos dotar de alta disponibilidad, aquí se puede entender como soluciones la memoria o puesta en marcha de dispositivos de hardware especializados. (Barrio, 2011, p.1).

Por lo general con el software que se utiliza para poder tener alta disponibilidad en los servidores no es suficiente, por lo tanto, toca hacer uso de herramientas o complementos adicionales para su configuración como, por ejemplo: corta fuegos, políticas de seguridad, etc. Las herramientas más importantes que se pueden mencionar dentro se los sistemas operativos GNU/Linuz se tiene Heartbeat, Ha-OSCAR, KeepAlived, Red Hat Cluster Site, The High Availability Linux Project, LifeKeeper o Veritas Cluster Server. (Barrio, 2011, p. 1-2).

Las máquinas paravirtualizadas Linux permiten un aumento en caliente del tamaño de la memoria, posibilitando así que los portales que puntualmente necesiten más recursos dispongan de ellos, ofreciendo así una adaptación dinámica y una mejor gestión de los recursos disponibles. (Prats, Vega y Cambras, 2008, p.85).

Los clústeres se han enfocado a poder ofrecer un entorno dedicado para los usuarios sin dejar de ofrecer una alta disponibilidad. Al implementarlo usando máquinas virtuales, estos usuarios se benefician de un servicio con valor añadido gracias a las características que ofrece la virtualización. (Prats, Vega y Cambras, 2008, p. 84).

### *1.3.2. Integridad*

Hoy en día la integridad en ámbitos de la virtualización tiene una gran importancia. Ya que la gestión de la integridad incluye la protección, medición, informes y verificación de la integridad de las máquinas virtuales. (Jansen, Ramasamy y Schunter, 2011, p. 3). De acuerdo a Jansen, Ramasamy y Schunter (2011). En un entorno de servidor (no virtualizado), los usuarios de hoy están convencidos de que sus servidores son confiables para:

- Ejecutar los servidores ellos mismos
- Pedir a un proveedor que garantice el control total sobre el servidor
- Pedirle a un proveedor que proporcione archivos de registro y otra evidencia que permita al usuario validar heurísticamente las instalaciones críticas, o
- Realización de auditorías periódicas de los servicios alojados.

La administración de integridad en un entorno virtualizado es aún más difícil debido a los desafíos únicos de seguridad y privacidad que surgen en dicho entorno. Los usuarios desean convencerse de que los servidores virtuales son tan seguros como los servidores físicos. Sin embargo, esto no es trivial, ya que la seguridad de los servidores virtuales no solo depende de la configuración del servidor, sino también de la seguridad del monitor de la máquina virtual (VMM) y de sus servicios y de la capacidad de garantizar un grado aceptable de no interferencia. Aislamiento entre máquinas virtuales. (Jansen, Ramasamy y Schunter, 2011, p. 3).

Además de poder demostrar la seguridad a un usuario, un requisito importante de privacidad es una garantía de que esta prueba no proporciona información sobre otros usuarios en el VMM. En particular, cuando los clientes de la competencia están alojados conjuntamente en el mismo hardware físico, hoy en día no existen “jaulas virtuales” que puedan garantizar su aislamiento verificable. De acuerdo a Jansen, Ramasamy y Schunter (2011). Para proporcionar tales garantías, varios aspectos de la VMM deben ser verificables y protegidos:

- El software del monitor de máquina virtual (VMM) debe diseñarse para satisfacer los requisitos de seguridad de un cliente.
- El software que se ejecuta en la máquina debe corresponder con una instalación correcta de un monitor de máquina virtual dado.

- Las políticas y los archivos de configuración utilizados por el VMM deben garantizar los requisitos de seguridad del cliente. Además, las políticas deben evitar la modificación no autorizada del software.

En la Figura 8-1 se puede visualizar una noción abstracta del modelo de integridad que se utiliza para poder monitorear las máquinas virtuales

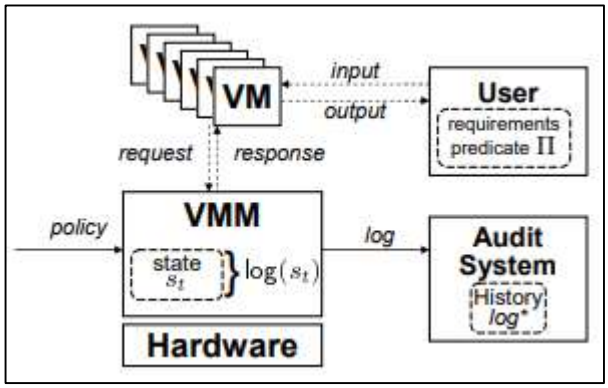



**Figura 8-1:** Modelo de integridad para el monitoreo de máquinas virtuales.
**Fuente:** Jansen, Ramasamy y Schunter; 2011, p. 4.

### *1.3.3. Confidencialidad*

La confidencialidad es un tema que posee múltiples significados dependiendo de cada autor, en el cual se refieren a la privacidad, en los cuales cada autor menciona su respectivo significado como se muestra a continuación: (Jiménez, 2013, p. 62)

- "La pro de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados". (Levina O., Oetting J. & Chou Y., 2011, citado en Jiménez, 2013, p. 62).
- "Mantener en secreto los datos de los usuarios en los sistemas de la nube." (Zhou M., Zhang R., Xie W., Qian W. & Zhou A., 2010, citado en Jiménez, 2013, p. 62).
- "La confidencialidad implica que los datos y las tareas de computación del cliente deben mantenerse confidenciales tanto del proveedor en la nube como de otros clientes." (Xiao Z. & Xiao Y., 2012, citado en Jiménez, 2013, p. 62).

Se puede decir que la confidencialidad es una característica de la privacidad a la información que se desea proteger en el que se establecen medidas de prevención para que no exista una divulgación de

datos no deseado. También se puede decir que la confidencialidad es un atributo de la privacidad. (Ma X., 2012.) Dando como una diferencia que la privacidad es un concepto global en la cual se contiene la protección, legislación, mientras que la confidencialidad es más específica con respecto a los datos que se desea proteger. (Jiménez, 2013, p. 62).

## 1.4. Vulnerabilidades en los sistemas de virtualización

Para poder conocer las vulnerabilidades que se tienen en los hipervisores, se ha realizado una investigación en una base de datos de vulnerabilidades que posee una buena reputación, conocido como Common Vulnerabilities and Exposures (CVE), en el cual se realiza un detalle de las vulnerabilidades más comunes que se tiene, los tipos más comunes de vulnerabilidades que se pueden encontrar en los hipervisores son Denegación de servicio (DoS), desbordamiento de pila , corrupción de memoria, recorrido de directorios y ganancia de información. (Litchfield y Shahzad, 2017, p. 2).

### *1.4.1. Tipos de ataques*

- **Denegación de servicio (DoS):** es un ataque el cual se encuentra destinado al consumo de los recursos de una manera exagerada que puede estar destinada para servidores o una red, para que los usuarios legítimos no puedan tener servicios de las mismas. En un ataque DoS, un servidor o red de destino se inundan con una gran cantidad de solicitudes formateadas. (Deshmukh, 2015, citado en Litchfield y Shahzad, 2017, p. 5).

  Por los resultados obtenidos en el primer trimestre de Kaspersky el ataque SYN aumento alcanzando un 84% lo cual representa al ataque de denegación de servicio más realizado. (Kaspersky, 2019).
- **Code Execution:** algunos sistemas de software permiten la carga de extensiones de archivos en un servidor web. Esto da como resultado la ejecución del código si un archivo es ejecutable, como *.asp, *.php, o *.shtml. (Christey y Martin, 2007, citado en Litchfield y Shahzad, 2017, p. 5).
- **Desbordamiento de pila:** se produce un desbordamiento exitoso cuando una función copia datos en un búfer sin realizar una comprobación de límites. (Christiansen, 2007, citado en Litchfield y Shahzad, 2017, p. 5).
- **Corrupción de la memoria:** el presente ataque existe cuando se encuentra errores en el código lo cual facilita al atacante el poder lanzar un ataque de corrupción, como por ejemplo, desbordamiento de bufer, daños en el montón y cadena de formato. Una explotación exitosa de

corrupción de memoria a menudo obliga a un programa a fallar. (Chen, Xu, Nakka, Kalbarczyk y Iyer, 2005, citado en Litchfield y Shahzad, 2017, p. 5).

- **Bypass Something:** omitir algo, como la autenticación, permite a un atacante obtener los mismos privilegios que los usuarios legítimos de un sistema. El atacante omite los procesos tanto de validación de entrada como el envío de entrada no válida a un servidor. Por ejemplo, una secuencia de comandos de sitios cruzados del lado del cliente se implementa para anular la validación de entrada. (Tajpour, Ibrahim y Sharifi, 2012, citado en Litchfield y Shahzad, 2017, p. 6).
- **Gain information:** la configuración del sistema o la vulnerabilidad del software se explota para exponer la información de acceso a la red o al sistema. Se realiza para poder obtener la información en ese mismo momento o en el futuro. (Litchfield y Shahzad, 2017, p. 6).
- **Gain privileges:** Obtener privilegios de alto nivel sin pasar por un proceso de autenticación. Después de explotar una vulnerabilidad del sistema, un atacante que haya obtenido acceso no autorizado al sistema puede ejecutar operaciones como un usuario autenticado. El acceso puede ser limitado si a los usuarios se les ha otorgado el menor privilegio disponible. (Provos, Friedl y Honeyman, 2003, citado en Litchfield y Shahzad, 2017, p. 6).

En la Tabla 2-1, se puede observar los ataques que se explicaron anteriormente, cuales son los más frecuentes en los diferentes hipervisores como son: VMWare, Xen y KVM.

**Tabla 2-1:** Vulnerabilidades de cada hipervisor.

| | **VMWare** | **Xen** | **KVM** | **Total** |
|---|---|---|---|---|
| **DoS** | 66 | 131 | 30 | 227 |
| **Code Execution** | 48 | 12 | 2 | 62 |
| **Desbordamiento de pila** | 30 | 28 | 4 | 62 |
| **Corrupción de la memoria** | 8 | 10 | 2 | 20 |
| **ByPass Something** | 5 | - | 3 | 8 |
| **Gain information** | 17 | 16 | 2 | 35 |
| **Gain Privileges** | 54 | 24 | 7 | 85 |
| **Total** | 228 | 221 | 50 | |

**Fuente:** Litchfield y Shahzad, 2017, p. 6.

**Realizado por:** Arias, Angel; 2019.

*1.4.1.1. Ataque de denegación de servicio distribuido (DDOS) SYN*

El ataque de denegación de servicio distribuido (DDOS) SYN es en donde los atacantes mandan una cantidad grande de paquetes hacia el servidor y utilizan totalmente sus recursos para que el usuario no tenga acceso.

El presente tipo de ataque se encuentra basado en el three whay handshake, en donde el servidor recibe una petición SYN, responde con un SYN+ACK, y el servidor espera que la computadora responda con un ACK para que empiece a existir la conexión, y posteriormente comenzar con una nueva conexión como se puede observar en la Figura 9-1 como se realiza la conexión con three whay handshake sin sufrir ataques. A diferencia como se puede observar en la Figura 10-1 en donde se observa como es el ataque de SYN com three whay handshake. (Singh, Garg y Kumar, 2012, p. 3).

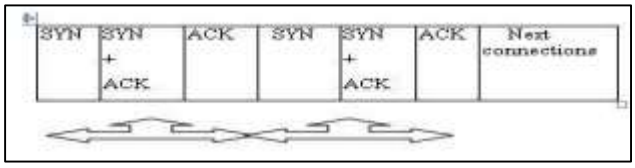



**Figura 9-1:** Conexión three whay handshake sin ataques.

**Fuente:** Singh, Deepak; Garg, Naveen; Kumar, Sushil; 2012, p. 3.

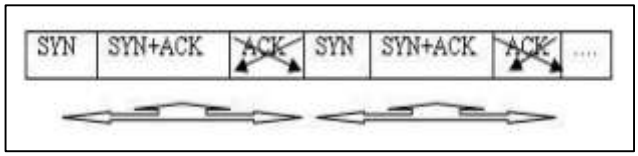



**Figura 10-1:** Conexión three whay handshake con ataque SYN.

**Fuente:** Singh, Deepak; Garg, Naveen; Kumar, Sushil; 2012, p. 4.

### *1.4.2. Metodologías*

Conociendo previamente que no existe una metodología en concreto para el análisis de vulnerabilidades de los servidores virtuales, se tomarán en cuenta las siguientes metodologías para poder realizar el análisis de vulnerabilidades:

*1.4.2.1. National Institute of Standards and Technology 800 – 144*

La metodología National Intitute of Standards and Technology (NIST) 800 – 144, es una guía destinada para tener en cuenta la seguridad y privacidad de Cloud Computing. El Cloud Computing ha sido definida por NIST como un modelo para permitir el acceso conveniente y bajo demanda de la red a un conjunto compartido de recursos informáticos configurables. Una de las grandes ventajas del Cloud Computing es que se pueden implementar en una amplia variedad de arquitecturas, bajo diferentes modelos de servicio e implementación, lo cual da la facilidad de poder coexistir con otras tecnologías y enfoques de diseño de software. (Jansen y Grance, 2011, p. 1).

La presente guía ha sido realizada con la finalidad de ser utilizada en agencias federales, también como en organizaciones no gubernamentales de forma voluntaria, la cual no está sujeto a derechos de autor, pero por respeto de desea que se reconozca la contribución. (Jansen y Grance, 2011, p. 1).

El propósito principal de la presente metodología es la de proporcionar una descripción general del Cloud Computing y los desafíos de seguridad y privacidad a los que se están enfrentando. La presente metodología se encarga de analizar las amenazas, riesgos tecnológicos y las salvaguardas para el Cloud Computing, y a la vez proporcionando información necesaria para poder tomar decisiones informadas sobre el tratamiento de la información de la tecnología. (Jansen y Grance, 2011, p. 1).

De acuerdo a Jansen y Grance (2011). La estructura en general que posee la presente metodología es la siguiente:

- Presentación de una visión general del Cloud Computing.
- Discusión de beneficios e inconvenientes de los servicios de Cloud Computing desde una perspectiva de seguridad y privacidad.
- Discute temas claves de seguridad y privacidad en Cloud Computing y las precauciones que se pueden tomar para mitigarlos.
- Proporciona orientación sobre cómo abordar los problemas de seguridad y privacidad cuando se subcontrata el soporte para datos y aplicaciones a un proveedor de la nube.

#### *1.4.2.2. Proyecto de Seguridad para Aplicaciones en Red Abierta (OWASP)*

En el Proyecto de Seguridad para Aplicaciones en Red Abierta (OWASP), estamos tratando de hacer del mundo un lugar donde el software inseguro sea la anomalía, no la norma. La Guía de Pruebas OWASP tiene un papel importante que desempeñar en la solución de este grave problema. Es de vital importancia que nuestro enfoque para pruebas de software por temas de seguridad se base en los

principios de ingeniería y ciencia. Necesitamos un enfoque consistente, repetible y definido para las pruebas de aplicaciones web. (OWASP, 2011, p. 8).

OWASP da a personas de seguridad con conocimientos afines, la capacidad de trabajar conjuntamente y formar un enfoque de práctica de liderazgo para un problema de seguridad. (OWASP, 2011, p. 8).

El objetivo que tiene el proyecto de pruebas OWASP es el de ayudar a las personas para que conozcan el qué, por qué, cuándo, dónde y el cómo de la prueba de las aplicaciones web. (OWASP, 2011, p. 8).

De acuerdo a OWASP (2011). Se encuentra organizada de la siguiente manera:

- Introducción. La cual cubre los requisitos de aplicaciones web y su alcance, asi como también los principios exitosos de pruebas y las técnicas de pruebas.
- Marco de pruebas de OWASP, explicando las técnicas y tareas en relación con las distintas fases del ciclo de vida del desarrollo de aplicaciones.
- Cómo comprobar vulnerabilidades especificas mediante inspección de códigos y pruebas de penetración.

#### *1.4.2.3. Information Systems Security Assessment Framework (ISSAF)*

La metodología conocida como Information Systems Security Assessment Framework (ISSAF) se encuentra destinada para poder evaluar la red en la que se esté conectado, así como los sistemas y aplicaciones de control. La presente metodología consiste en tres fases de aproximación y nueve pasos de evaluación, en el cual el enfoque incluye las siguientes tres fases: (OISSG, 2006, p. 13)

- Fase 1: planificación y preparación.

En esta fase se tiene los pasos iniciales para el intercambio de información, se planea y se prepara para el test. Antes de realizar cualquier prueba, primero se firmará un acuerdo entre ambas partes para protección legal mutua. A la vez se especificará el equipo a utilizar, las fechas exactas, las horas que se realizarán las pruebas, la/s ruta/s de camino y otros arreglos. Las siguientes actividades se tienen previstas que se realicen en esta fase: (OISSG, 2006, p. 13).

I. Identificación de contactos de ambas partes.
II. Reunión para definir el alcance, enfoque y metodología.
III. Aceptación de las pruebas específicas y la/s ruta/s de camino.

- Fase 2: evaluación.

En esta fase se realiza el test de penetración, esta fase se encuentra dividido en nueve pasos como se puede observar en la Figura 11-1 (OISSG, 2006, p. 13). De acuerdo a OISSG (2006), a continuación, se mencionan los nueve pasos que son:

I. Obtención de la información.
II. Mapeo de la red.
III. Identificación de vulnerabilidades.
IV. Penetración.
V. Ganancia de acceso y escalabilidad de privilegios.
VI. Enumeración.
VII. Compromiso remoto de los usuarios y sitios.
VIII. Mantener el acceso.
IX. Cubrir las pistas.

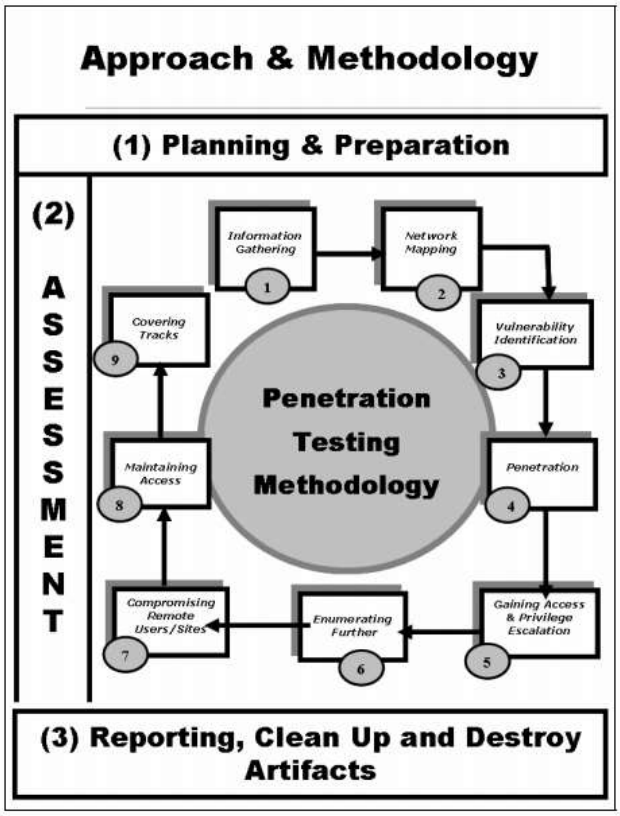



**Figura 11-1:** Metodología en fases y pasos de ISSAF.

**Fuente:** OISSG; 2006, p. 14.

- Fase 3: reportaje, limpieza y destrucción de artefactos.

#### *1.4.2.4. Open Source Security Testing Methodology Manual (OSSTMM)*

La metodología Open Source Security Testing Methodology Manual (OSSTMM) es un test en el cual se necesitará realizar un seguimiento de las pruebas, como realiza el test, los tipos de controles descubiertos y cuales no probo. (ISECOM, 2011, p. 2) Es una metodología que sirve para evaluar la seguridad de localizaciones físicas, interacciones humanas y todas las formas de comunicación existentes (Wireless, Cableadas, Analógicas y Digitales). (López, 2015, p. 17).

OSSTMM es una guía para mejorar la seguridad en los equipos informáticos, la presente metodología se divide en canales, módulos, ambientes, fases según sea la prueba de seguridad que se desea realizar. (Cruz y Martínez, 2017, p. 506). De acuerdo a López (2015). Esta metodología evalúa la seguridad desde todos los puntos de vista, los cuales son:

I. Humano.
II. Físico.
III. Wireless.
IV. Telecomunicaciones.
V. Redes de datos.

Además, esta tecnología posee de métricas y explica cómo hay que realizar los informes. Tampoco cuenta con una guía técnica sobre cómo llevar a cabo las pruebas que propone, pero es precisamente este el objetivo del presente trabajo con lo que tampoco se considera un aspecto negativo. (López, 2015, p. 18).

De acuerdo a López (2015). La realización de una auditoria con la metodología de OSSTMM asegura lo siguiente:

- Se han realizado las pruebas de forma exhaustiva.
- Las pruebas incluyen todos los ámbitos necesarios.
- Las pruebas entran dentro de la regulación actual del país.
- Los resultados pueden medirse de forma cuantitativa.
- Los resultados son consistentes y se pueden medir. (López, 2015, p. 24)

### *1.4.3. Hipervisores Open Source*

Los hipervisores más importantes que se tienen en Open Source son:

*1.4.3.1. Xen*

Xen trabaja introduciendo un software muy pequeño, muy compacto y enfocado que se ejecuta directamente en el hardware y proporciona servicios a los sistemas operativos virtualizados. (Takemura Crawford, 2003, p. 5).

El enfoque de Xen para la virtualización elimina la mayor parte de la división entre el sistema operativo host y el sistema operativo invitado. La virtualización completa y la virtualización a nivel del sistema operativo tienen una clara distinción: el sistema operativo host es el que se ejecuta con privilegios completos. Con Xen, solo el hipervisor tiene privilegios completos, y está diseñado para ser lo más pequeño y limitado posible. (Takemura y Crawford, 2003, p. 5).

El hipervisor funciona como el núcleo de un sistema operativo tradicional, parcelando el tiempo de CPU y los recursos a los sistemas operativos que se ejecutan bajo él, que a su vez asignan recursos a sus procesos individuales. Al igual que los sistemas operativos modernos pueden pausar un proceso de manera transparente, el hipervisor Xen puede pausar un sistema operativo, controlar manualmente a otro por un tiempo y luego reiniciar sin problemas el sistema pausado. (Takemura y Crawford, 2003, p. 6)

El equipo de Xen lo define como un hypercall, los cuales reemplazan a las llamadas al sistema de un sistema operativo estándar, con una interfaz similar. En efecto, tienen la misma función: permitir que el código de usuario ejecute operaciones privilegiadas de una manera que puede ser controlada y administrada por un código de confianza. (Takemura y Crawford., 2003, p. 6).

Los hypercalls tienen varios objetivos y requisitos de diseño. Primero, son asíncronos para que las hypercalls no bloqueen otros procesos u otros sistemas operativos, mientras que un dominio espera a que finalice una hypercall, otro dominio puede obtener algo de tiempo de CPU. En segundo lugar, son pequeños, simples y claramente definidos: Xen tiene solo unos 50 hypercalls, en contraste con más de 300 syscalls para Linux. Finalmente, las hypercalls usan un sistema común de notificaciones para interactuar con el hipervisor Xen. (Takemura y Crawford, 2003, p. 6).

De acuerdo a Hurtares, Camino y Durango (2012). Una de las ventajas que ofrece XenServer es la de soportar balanceo a nivel de origen, lo cual lo realiza de la siguiente manera:

- Usa modo activo/activo, por lo cual solo soporta el balanceo de carga para el tráfico de las VMs a través de las NICs, esto se realiza basado en el paquete de la dirección MAC.
- Ofrece un servicio de failover para todos los demás tipos de tráficos.
- No es necesario que el switch soporte 802.3ad, agregación de enlaces paralelos (Trunking).
- Es derivado del modo Adaptive Load Balancing (ALB), el cual ofrece un incremento del ancho de banda lo cual permite la transmisión sobre 2 – 8 puertos hacia múltiples direcciones de destino.
- Incorpora Adapter Fault Tolerance, lo cual permite balancear la carga a través de las interfaces, dicho rebalanceo se realiza cada 10 segundos. (Hurtares, Camino y Durango, 2012, p. 5).

#### *1.4.3.2. KVM*

El hipervisor KVM se incluye en las principales versiones de GNU / Linux, ya que se ha convertido en el hipervisor de elección dentro de la comunidad de GNU / Linux, por lo que está disponible en los diversos repositorios de distribución. De hecho, KVM es un módulo de kernel de GNU / Linux que permite que los programas dentro del espacio del usuario accedan a las funciones de virtualización del procesador Intel o AMD. Como resultado, las máquinas virtuales KVM (VM) realmente se ejecutan como procesos de espacio de usuario. KVM usa QEMU, un emulador de máquina de código abierto y genérico y virtualizador para la emulación de hardware de entrada y salida. (Diarmund, 2017, p. 9).

Puede emular una variedad de procesadores en un procesador invitado y, combinado con el módulo de kernel KVM, puede alcanzar velocidades nativas. Se admiten todas las combinaciones de sistemas de host e invitados de 32 y 64 bits, excepto los invitados de 64 bits en los hosts de 32 bits. (Diarmund, 2017, p. 9).

KVM es un hipervisor de tipo 1 y tipo 2 que se ejecuta directamente en hardware x86. La interfaz de GNU / Linux hace que parezca que se trata de un hipervisor alojado que se ejecuta en ella, pero, de hecho, cada máquina virtual se está ejecutando de manera simple. El sistema operativo GNU / Linux del host proporciona un launchpad para el hipervisor y luego se involucra en un coprocesamiento. Relación con el hipervisor. En la Figura 12-1 se puede visualizar un esquema de la virtualización de KVM. (Diarmund, 2017, p. 9).

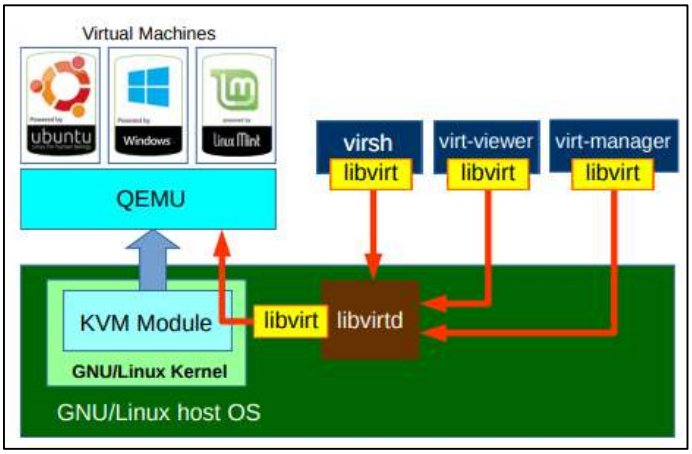



**Figura 12-1:** Diagrama de bloque de la virtualización de KVM.

**Fuente:** Diarmund; 2017, p. 9.

De acuerdo a Gómez (2012). Las mayores ventajas que presenta KVM son las siguientes:

- Está diseñado para procesadores x86, centrando en una virtualización total.
- No se modifica el kernel de GNU/Linux.
- Solamente es un módulo que no necesita parches.
- Contiene soporte de paravirtualización.
- KVM funciona en todo tipo de máquinas, servidores, escritorio o laptop.
- Migración en caliente de máquinas virtuales.
- Tiene administración vía web, gráfica y consola.
- Las administraciones de las máquinas virtuales se hacen por medio de un usuario mortal.
- Podemos utilizar el comando kill para matar maquina virtuales ya con KVM son reconocidos como procesos.
- Maneja 3 tipos de configuración de red, "Bridge, Route, NAT".
- Permite ejecutar múltiples máquinas virtuales cada una con su propia instancia. (Gómez, 2012, p. 3).

*1.4.3.3. Oracle VirtualBox*

Oracle VirtualBox es una de las plataformas de simulación para tener varias máquinas virtuales en un mismo ordenador. De acuerdo a Oracle (2019). Las características más útiles son para los siguientes escenarios:

- Ejecución de múltiples sistemas operativos al mismo tiempo. De esta manera se puede utilizar softwares diferentes por ejemplo en Windows se puede utilizar Linux o Mac, sin tener que reiniciar el dispositivo. A la vez presenta una gran ventaja ya que permite instalar un sistema operativo antiguo, aunque el dispositivo no sea compatible con dicho sistema operativo.
- Fácil instalación de sistemas operativos. Instalar una solución completa para una empresa puede resultar difícil, con Oracle VirtualBox puede empaquetarse en una máquina virtual, por ejemplo, en el cual puede ser muy fácil como instalar y ejecutar un servidor de correo electrónico se vuelve una tarea más fácil.
- Pruebas y recuperación ante problemas. Cuando ya se han instalado las máquinas virtuales, los discos duros virtuales se pueden considerar como un contenedor el cual se puede congelar, copiar, respaldar, realizar una copia de seguridad y transportar la información que se tenga entre varios hosts.

  A la vez otra característica que presenta es que permite guardar un estado particular de una máquina virtual y volver a ese estado en caso de que sea necesario. Lo cual permite estar realizando varias pruebas, y en el caso de que se dañe alguna configuración se pueda volver fácilmente a un instante anterior, lo cual evita la necesidad de crear copias de seguridad de las máquinas virtuales. (Oracle, 2019, p. 2).

## 1.5. Top ten de OWASP

De acuerdo a OWASP Top 10 (2017). En el top ten de OWASP se tienen las siguientes vulnerabilidades que son las más dañinas que pueden sufrir las aplicaciones web:

**Tabla 3-1:** Top ten de OWASP.

| Vulnerabilidades | Significado |
|---|---|
| Inyección | Las fallas de inyección como SQL, NoSql, OS o LDAP ocurre cuando se envían datos no confiables a un intérprete, en el cual el atacante puede engañar al interprete para ejecutar comandos involuntarios. |
| Pérdida de autenticación | El atacante tiene la posibilidad de comprometer usuarios y contraseñas, tokens de sesiones o explotar otras fallas de implementación para asumir la identidad de otros usuarios. |

| | |
|---|---|
| Exposición de datos sensibles | Los atacantes pueden atacar o modificar datos como información financiera, de salud o personal. En el cual se pueden llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. |
| Entidades externas XML (XXE) | Las entidades externas pueden utilizarse para revelar archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar códigos de forma remota y realizar ataques de denegación de servicio (DOS). |
| Pérdida de control de acceso | Los atacantes pueden explotar los defectos que tienen para acceder de forma no autorizada a funcionalidades y/o cuentas de otros usuarios. |
| Configuración de seguridad incorrecta | Se debe en parte a establecer la configuración de forma manual, ad hoc o por omisión. Por ejemplo: cabeceras HTTP mal configuradas, falta de parches y actualizaciones, dependencias y componentes desactualizados, etc. |
| Secuencia de comandos en sitios cruzados (XSS) | Ocurre cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación adecuada. Permite ejecutar comandos en el navegador de la víctima y el atacante puede obtener una sesión, modificar los sitios web o re direccionar al usuario a un sitio malicioso. |
| Deserialización Insegura | Ocurre cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios. |
| Componentes con vulnerabilidades conocidas | Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor, en el cual se puede debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos. |
| Registro y monitoreo insuficientes | Permite al atacante mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. |

**Fuente:** Owasp top 10, 2017, p. 6

**Realizado por:** Arias, Angel; 2019.

## 1.6. Analizadores de vulnerabilidades

Entre los analizadores de vulnerabilidades que tienen en cuenta los parámetros del Top Ten de Owasp se tienen los siguientes:

### *1.6.1. OWASP ZAP*

OWASP Zed Attack Proxy (OWASP ZAP) es una herramienta gratuita que realiza el análisis de vulnerabilidades de forma dinámica. A la vez forma parte del grupo de proyectos de la fundación OWASP. Es muy utilizado ya que ofrece una gran cantidad de documentación y soporte, por ello es considerado uno de los escáneres de vulnerabilidades web gratuitos más populares.

El diseño y configuración permite ser usado tanto por personas expertas que poseen un alto grado de conocimiento, así como también por desarrolladores o personas sin tantos conocimientos. Es utilizado como un escáner automático, pero a la vez presenta una serie de herramientas individuales que facilitan las búsquedas de vulnerabilidades de forma manuales.

De acuerdo a García y Sandoval (2017). Los tipos de escaneos que se pueden realizar con OWASP son:

- Escaneo activo: es el más utilizado porque realiza un análisis completo por defecto de la aplicación en búsqueda de vulnerabilidades.
- Escaneo pasivo: etiqueta de manera automática las respuestas por parte de la aplicación web, en el que se tiene en cuenta reglas específicas. La herramienta no realiza ningún análisis intrusivo.
- Complementos: soporta la instalación de complementos para agregar mayor funcionalidad a la herramienta.
- Alertas: diferenciación con colores los diferentes tipos de alertas según su gravedad que puede ser alta, media, baja, información, falso positivo.
- API: OWASP ZAP provee un API a través del cual se puede interactuar con la herramienta mediante programación, los lenguajes de programación que soporta son: json, html y xml.
- Contexts: permite asociar diferentes tipos de URL’s con un mismo sitio.
- Data Driven Content: a la par de la utilización de los contextos, se reduce el número de peticiones en una misma página de un sitio.
- Filtros: con la utilización del proxy, se puede realizar filtros sobre cada petición y respuesta.
- Proxy interceptor: permite ver y almacenar un registro de todas las peticiones que se hacen hacia una aplicación web y sus respectivas respuestas.

- Reglas: soporta reglas para análisis activo o pasivo, todas las reglas que utiliza OWASP ZAP son complementos propios de las herramientas.
- Alcance: permite determinar el alcance de búsqueda de la aplicación, utilizando el grupo de URL's relacionadas. Por defecto el alcance es nulo, es decir, no tiene límite. (Owasp Top 10 – 2017, 2017, p.24 – 27).

### *1.6.2. Acunetix*

El escáner de vulnerabilidades web Acunetix, es una aplicación web pagada que permite analizar las vulnerabilidades que tienen las aplicaciones web tales como: SQL Injections, Cross site scripting y otras vulnerabilidades que pueden ser explotadas teniendo en cuenta el top ten de OWASP. Acunetix puede escanear sitios o aplicaciones web que usen el protocolo HTTP/HTTPS. (Acunetix Ltd., 2011, p. 8)

Acunetix es adecuado para utilizar en cualquier organización pequeña, mediana y grande con intranets, extranets y sitios web destinados intercambiar y/o entregar información con/a clientes, proveedores, empleados y otras partes interesadas. (Acunetix Ltd., 2011, p. 8).

### *1.6.3. W3af*

W3af es una herramienta de auditoria web OpenSource disponible tanto en Windows como en Linux. Se puede usar tanto desde una interfaz de usuario como desde la línea de comandos. El objetivo que tiene W3af es el de crear un framework para encontrar y ejecutar vulnerabilidades en aplicaciones web. (Alonso, Díaz, Guzmán, Laguna y Bailón, 2012, p.14).

La característica principal que tiene W3af es que su sistema de auditoria está basado completamente en plugins que se encuentran escritos en Phyton, gracias a ello consigue crear un framework fácilmente escalable y una comunidad que contribuyen con la programación de nuevos plugins ante los fallos de seguridad web que pueden ir apareciendo. (Alonso, Díaz, Guzmán, Laguna y Bailón, 2012, p.14).

### *1.6.4. Nikto*

Nikto es una herramienta de escaneo de servidores web. De acuerdo a López y Ramirez (2018) Nikto realiza diferentes actividades como:

- Detección de malas configuraciones y vulnerabilidades en el servidor objetivo.
- Detección de ficheros en instalaciones por defecto.
- Listado de la estructura del servidor, las versiones y sus respectivas actualizaciones.
- Tests de vulnerabilidades XSS
- Reportes en formato txt, csv, html, etc. (López y Ramirez, 2018, p. 4)

Una de las características más importantes que posee este analizador es la integración con LibWhiskeri, Metasploit, entre otras. Se encuentra bajo GNU/GPL lo que indica el código a disposición para usar, modificar y/o distribuir. (Seguridad Máxima, 2017, citado en López y Ramirez, 2018, p.4)

Cuando se utiliza la interfaz es necesario especificar el Host (dirección del servidor en donde se encuentra la aplicación), formato del reporte a generar que puede ser .csv, .txt y .html, nombre del reporte y directorio donde se desee guardar. (Seguridad Máxima, 2017, citado en López y Ramírez, 2018, p.4 – 5) Si se realiza mediante línea de código se puede observar a continuación la línea de código de cómo utilizar: "–h host 10.58.4.11 –Format .csv –o F:\Pruebas\reporte1.csv". Según López y Ramírez (2018) cada parámetro significa la siguiente

- -h es el host
- -Format es el formato en el que deseamos que se genere el reporte que puede ser .csv, .txt y .html
- -o se ubica la dirección y el nombre con la que se desea que se genere el reporte. (Seguridad Máxima, 2017, citado en López y Ramírez, 2018, p.4 – 5)

Basándonos en el estudio realizado en la tesis: "PROPUESTA DE UN MÉTODO UTILIZANDO TÉCNICAS DE PROGRAMACIÓN SEGURAS PARA EL DESARROLLO DE APLICACIONES WEB EN ENTORNOS PHP PARA MITIGAR RIESGOS POTENCIALES DE SEGURIDAD", se toma el estudio comparativo que se tiene entre los analizadores de vulnerabilidades anteriormente mencionados, en el cual se tiene en cuenta los siguientes puntos en la escala de Likert como se puede observar en la Tabla 4-1:

**Tabla 4-1:** Escala de Likert para comparar los analizadores de vulnerabilidades.

| | **Siempre** | **Casi siempre** | **Algunas veces** | **Muy Pocas veces** | **Nunca** |
|---|---|---|---|---|---|
| **Ítems positivos** | 5 | 4 | 3 | 2 | 1 |

**Fuente:** Monar, 2017, p. 42

**Realizado por:** Arias, Angel; 2019.

**Tabla 5-1:** Pesos asignados en los analizadores de vulnerabilidades.

| **Vulnerabilidades** | **Acunetix** | **OWASP ZAP** | **W3af** | **Nikto** |
|---|---|---|---|---|
| Inyección | 5 | 4 | 3 | 4 |
| Pérdidas de autenticación y gestión de sesiones | 5 | 5 | 4 | 3 |
| Secuencia de comandos en sitios cruzados (XSS) | 4 | 4 | 3 | 4 |
| Configuración de seguridad incorrecta | 3 | 3 | 3 | 3 |
| Exposición de datos sensibles | 4 | 3 | 3 | 3 |
| Falsificación de peticiones en sitios cruzados (CSRF) | 5 | 4 | 3 | 4 |
| Redirecciones y envíos no validos | 4 | 3 | 3 | 3 |
| **TOTAL** | **30** | **26** | **22** | **24** |

**Fuente:** Monar. 2017, p. 43

**Realizado por:** Arias, Angel; 2019

En la Tabla 5-1 podemos observar que el mejor analizador de vulnerabilidades es Acunetix, pero en la presente tesis se utilizó OWASP ZAP porque es de licenciamiento libre a comparación de Acunetix que es pagado y porque en la metodología que se utiliza de OWASP recomiendan la utilización de su propio escáner para identificar los problemas y soluciones que pueden tener las aplicaciones web.

## CAPÍTULO II

## 2. MARCO METODOLÓGICO

Para el presente trabajo de titulación se utilizó, la guía propuesta en el objetivo número 3. A la vez de comprobar la eficiencia de la guía de vulnerabilidades en el cual se utilizaron las siguientes fases:

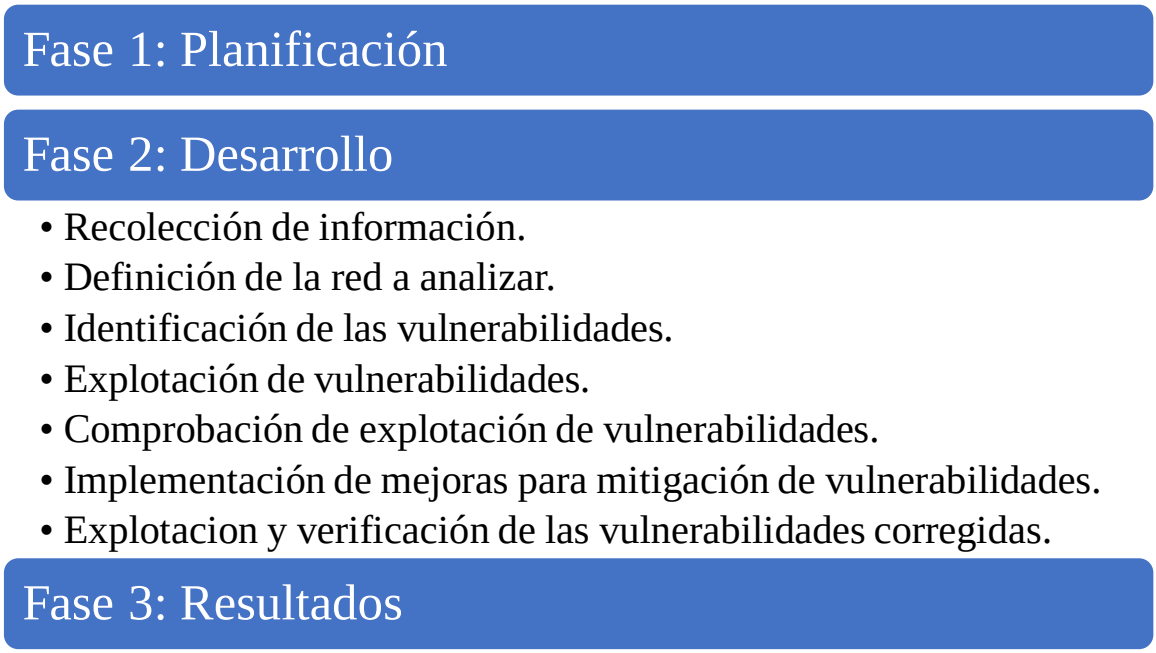



**Gráfico 1-2:** Etapas para el análisis de vulnerabilidades de servidores virtuales.

**Realizado por:** Arias, Angel; 2019, p.2.

En el siguiente diagrama de flujo se puede observar de manera más detallada la secuencia de pasos que se realizó para el presente trabajo de titulación:

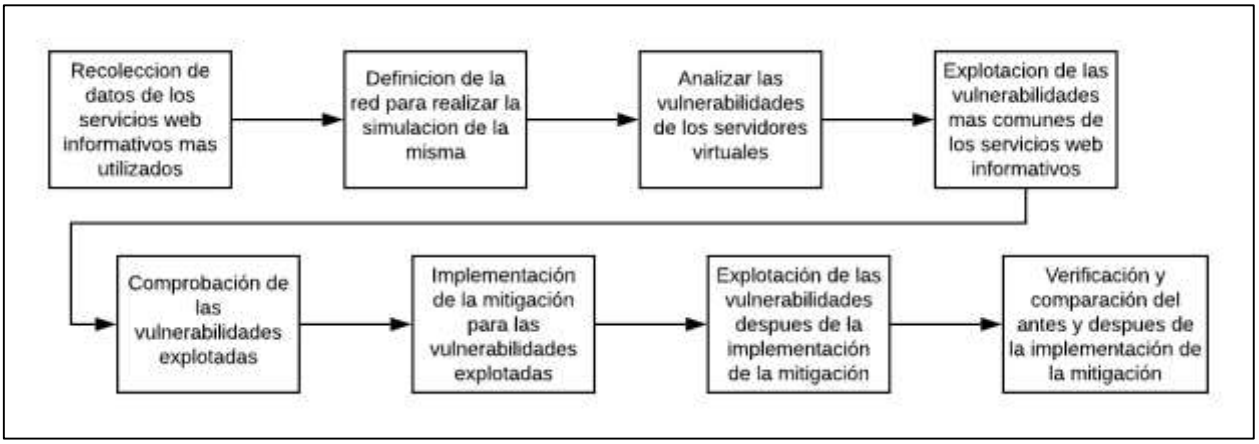



**Gráfico 2-2:** Secuencia de pasos de la realización del presente trabajo de titulación.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 1-2 se puede observar la secuencia de pasos que se seguirá en el presente trabajo de titulación, las etapas a realizar que se encuentra de manera más detalla en la guía de soluciones. En el Gráfico 2-2 se observa la secuencia de pasos que se realizó en el presente trabajo de titulación siguiendo las etapas anteriormente mencionadas en el Gráfico 1-2, dichas etapas se explicaran de forma más detalla a continuación:

## 2.1. Recolección de información

En la primera etapa se realizó tanto los oficios para acceder a información necesaria tanto en la Dirección de Tecnologías de la Información y Comunicación (DTIC) como en secretaria académica, como se puede observar en los Anexos A y B, en donde se realizo la encuesta que se encuentra en el Anexo D, con la finalidad de conocer principalmente los servicios web informativos de la ESPOCH más utilizados por los estudiantes para la correspondiente simulación de los mismos, en el cual gracias a los datos proporcionados por sercretaria académica de la ESPOCH se conoce que se tiene matriculado un numero de 18 732 estudiantes en el periodo de 6 Marzo – 26 Julio 2019 como se observa en el Anexo C. En la ecuación 1-2 se observa la formula que se utiliza para conocer la cantidad de encuestas que se debe realizar, mediante la formula de una muestra finita:

$$n = \frac{Z^2 * N * p * q}{e^2 * (N-1) * (Z^2 * p * q)}$$

**Ecuación 1-2**

- n es el tamaño de la muestra.
- Z es el nivel de confianza, el valor es de acuerdo a la siguiente tabla:

**Tabla 1-2:** Valores de confianza tabla Z.

| Valores de confianza tabla Z | |
|---|---|
| 90% | 1.65 |
| 91% | 1.7 |
| 92% | 1.76 |
| 93% | 1.81 |
| 94% | 1.89 |
| 95% | 1.96 |

**Realizado por:** Arias, Angel; 2019.

- p es el porcentaje de la población que tiene el atributo deseado.
- q es el porcentaje de la población que no tiene el atributo deseado es decir q=1-p.
  Nota: cuando no existe indicaciones de la población que posee o no el atributo, se asume 50 % para p y 50% para q.
- N es el tamaño del universo.
- e es el error de estimación máximo aceptado

Para el presente trabajo de titulación se utilizaron los siguientes datos para el cálculo de la muestra:

**Tabla 2-2:** Datos para cálculo de la muestra.

| | |
|---|---|
| Z | 1.96 |
| p | 50% |
| q | 50% |
| N | 18732 |
| e | 5% |

**Realizado por:** Arias, Angel; 2019.

En donde con la utilización de la Ecuación 1-2 y de los datos anteriormente mencionados en la Tabla 2-2, el valor de "n", es decir, la muestra para realizar las encuestas es de 377 estudiantes. Los datos que se obtiene después de la realización de la encuesta son:

- Facultad de los estudiantes encuestados, para comprobar se realizó en toda la ESPOCH.
- Los sistemas operativos más utilizados por los estudiantes de la ESPOCH.
- Desde qué dispositivo utilizan más frecuentemente los servicios web informativos de la ESPOCH.

- Cuáles son los servicios web informativos de la ESPOCH más utilizados por los estudiantes.
- Como califican los estudiantes los servicios web informativos de la ESPOCH.
- Conocimiento de los estudiantes sobre la seguridad que poseen los servicios web informativos de la ESPOCH.
- Como protegen los estudiantes su información cuando acceden a los servicios web informativos.
- Toman los estudiantes las medidas adecuadas de seguridad cuando acceden a los servicios web informativos.
- Son satisfactorios para los estudiantes los servicios web informativos de la ESPOCH.
- La frecuencia en la que los estudiantes utilizan los servicios web informativos.
- Qué tipo de conexión es la más utilizada para utilizar los servicios web informativos de la ESPOCH.

## 2.2. Definición de la red a analizar

A la par que obtienen los datos anteriormente mencionados con la encuesta en el Anexo D, el DTIC de la ESPOCH proporcionó datos como el sistema operativo en el que corren las páginas web informativas el cual es joomla. Por motivos de políticas que posee el DTIC no se facilitó las direcciones IP de las redes ni el enrutamiento con el que se encuentra configurado la red, tampoco como se encontraban los servidores configurados, así como tampoco los datos de ancho de banda o las características que poseen los servidores con los servicios web informativos.

En la figura 1-2 se puede observar las características de la computadora a utilizar para el presente trabajo de titulación. En donde se da mayor prioridad tanto a la máquina virtual atacante que se encuentra en Kali Linux como a los servidores que utilizan CENTOS 7.

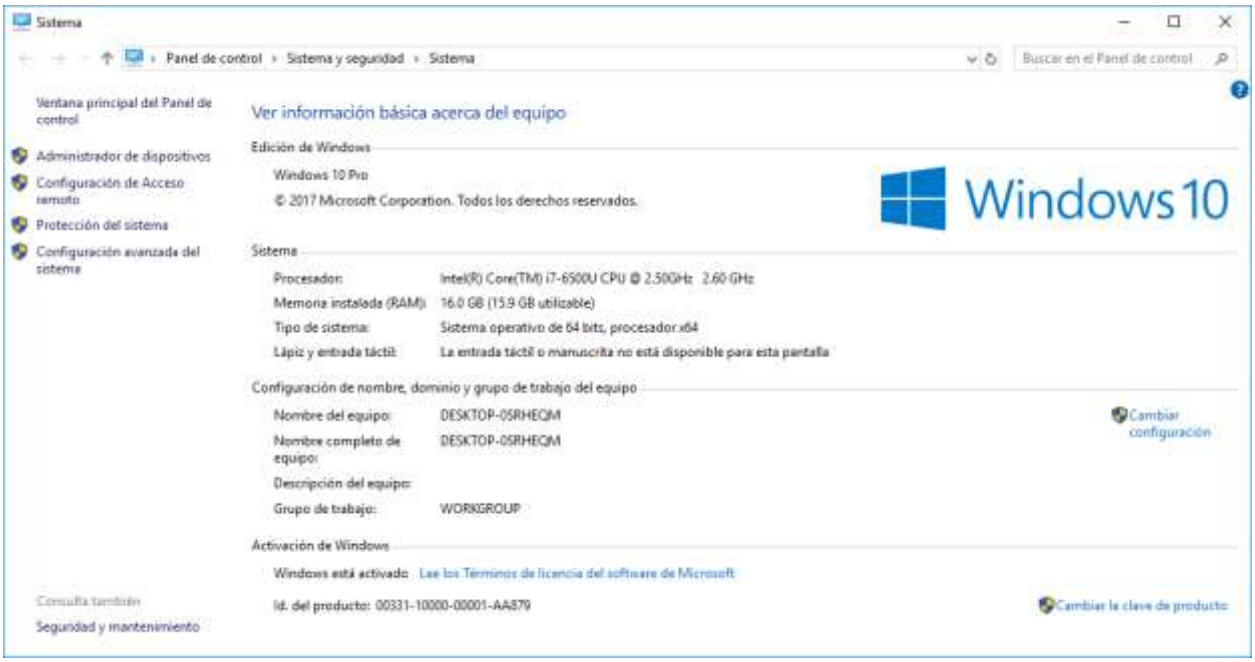



**Figura 1-2:** Características del computador.

**Realizado por:** Arias, Angel; 2019.

En la Figura 1-2 se puede observar las características que posee el computador que se utilizó en la realización del presente trabajo de titulación, en donde, se tienen las siguientes características más importantes que posee:

- 16 GB de RAM.
- Procesador Intel(R) Core(TM) i7-6500U CPU @ 2.50 GHz 2.60 GHz.
- Sistema operativo de 64 bits, procesador x64.
- Sistema operativo Windows 10 Pro.

Teniendo en cuenta todos los parámetros que facilitó el DTIC y el grupo de investigación SEGINTE "SEGURIDAD DE LA INFORMACIÓN Y TELEMÁTICA" en función del proyecto: "Propuesta de Solución SDN – Sistema de Aprendizaje para identificación y clasificación de amenazas internas que mejoren el control y la seguridad en intranets académicas.", facilitó la siguiente topología de red la cual es muy parecida a un nodo de red de la ESPOCH, no se trabaja con uno completamente similar por motivos de confidencialidad:

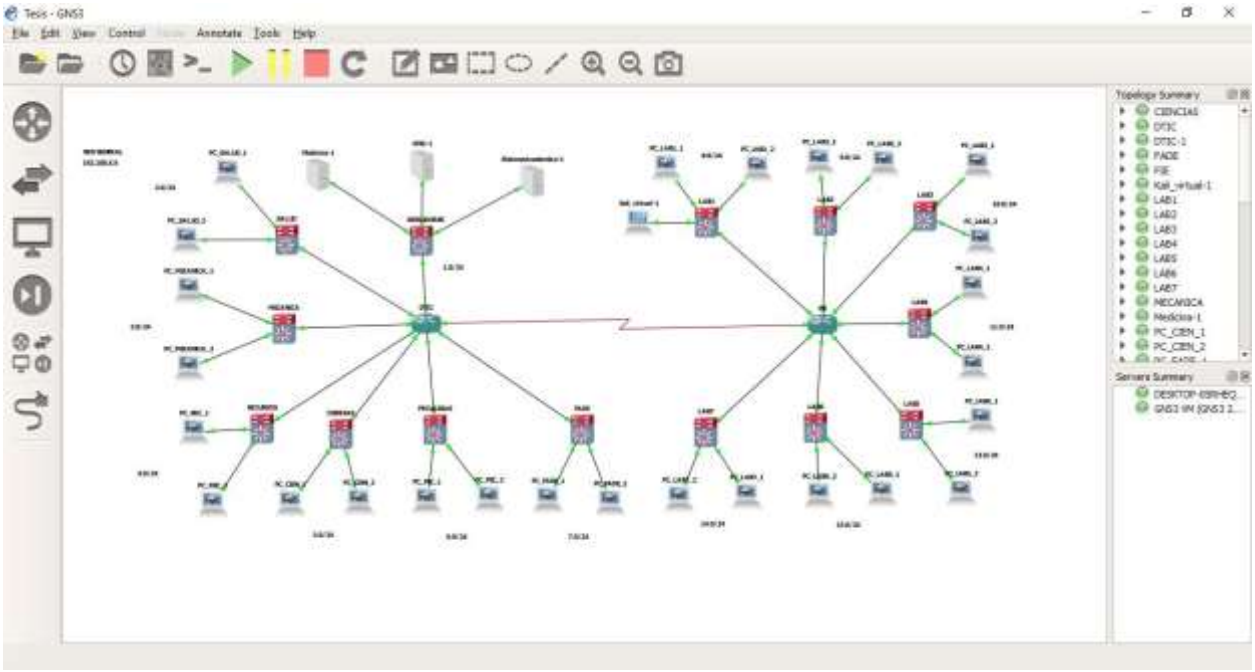


**Figura 2-2:** Escenario de la red simulada.

**Realizado por:** Arias, Angel; 2019.

En el escenario que se puede observar en la Figura 2-2 se utilizó para el enrutamiento el protocolo OSPF con el direccionamiento que se observa en el Anexo F, los tres servidores a simular y analizar son:

- Sistema web institucional
- Sistema e-Salud ESPOCH
- DTIC

Se escogieron los tres servicios web informativos antes mencionados por los resultados que se pueden observar en la Figura 4-3. Las características que tienen los tres servidores virtuales son los que se pueden observar en la Figura 3-2 y en la Figura 4-2.

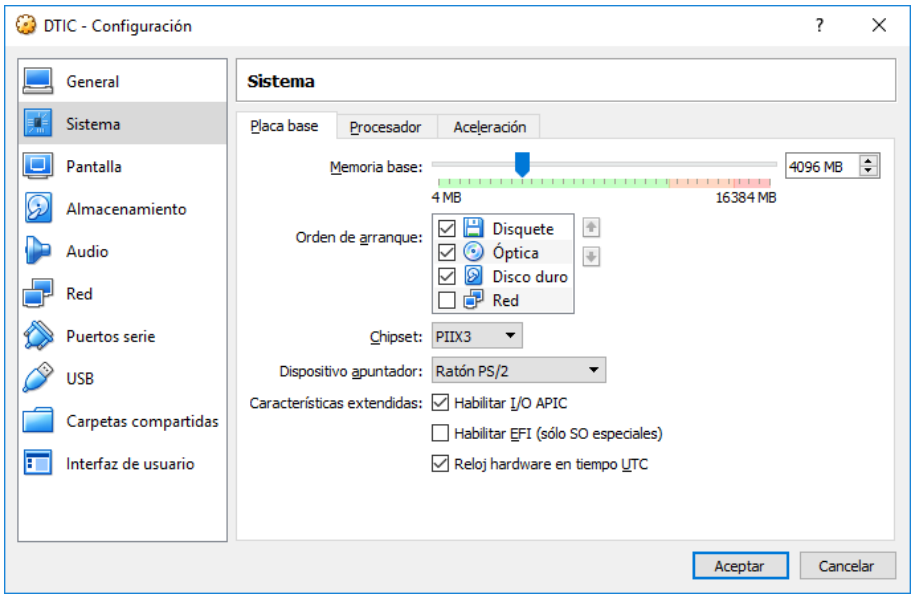



**Figura 3-2:** Memoria RAM de los servidores.

**Realizado por:** Arias, Angel; 2019.

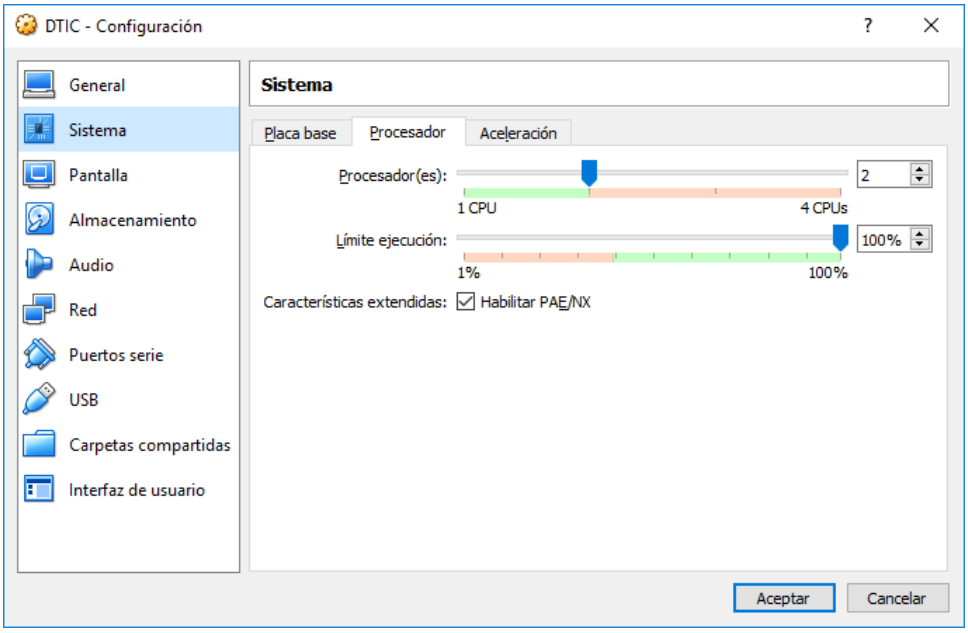



**Figura 4-2:** Procesadores de los servidores.

**Realizado por:** Arias, Angel; 2019.

En la Figura 3-2 y Figura 4-2 se observa la cantidad de memoria RAM y el número de procesadores que utilizan los servidores virtuales correspondientemente, los cuales el sistema operativo en el que se encuentran es CENTOS 7 de distribución gnu/Linux.

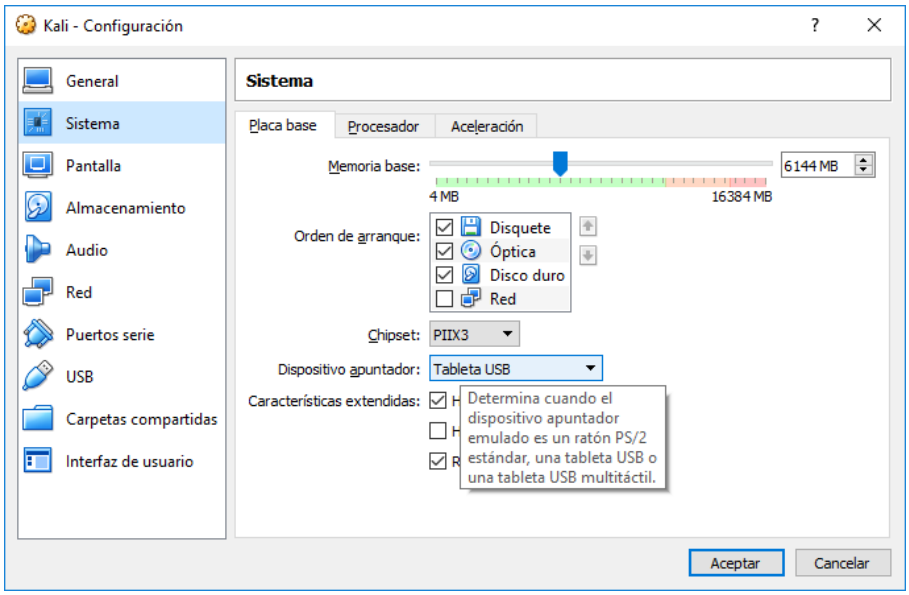



**Figura 5-2:** Memoria RAM de la computadora atacante.

**Realizado por:** Arias, Angel; 2019.

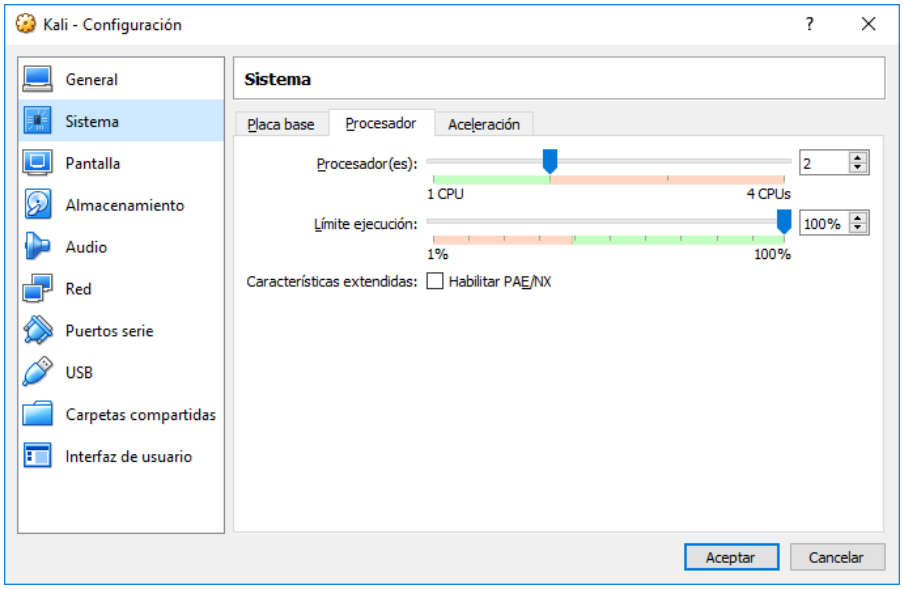



**Figura 6-2:** Número de procesadores de la computadora atacante.

**Realizado por:** Arias, Angel; 2019.

En las Figuras 5-2 y 6-2 se puede observar las características que utiliza la computadora atacante con sistema operativo de Kali Linux, en donde se puede observar que utiliza 6 GB de RAM y dos procesadores al máximo del límite de ejecución.

Los presentes parámetros tanto de la computadora atacante como de los servidores no se les da una mayor capacidad de memoria RAM o número de procesadores ya que la computadora en donde se realiza la simulación debe tener los recursos necesarios para correr a la vez los servidores, la maquina atacante, el simulador GNS3, entre otros programas que se necesitan. Por tal motivo en el momento de la realización de las pruebas se analizó los servidores por separado para que puedan tener mayor cantidad de recursos y obtener los datos más óptimos.

Para la configuración de los servidores se siguieron los siguienes pasos:

- Instalación del sistema operativo Centos 7 y Kali Linux

En primer lugar, se realiza la instalación de los sistemas operativos de Centos 7 para utilizarlo en los servidores y de Kali Linux para la utilización de la máquina virtual como atacante. Cada una de las imágenes se instaló con configuración por defecto.

- Instalación y configuración de joomla

En segundo lugar, se descarga e instala joomla en cada uno de los servidores como se puede observar en el Anexo G, así como se puede observar a la vez la instalación en las figuras 3-12 a 3-16. Después de tener instalado joomla se descarga una plantilla y se configura la página web informativa como se desea, la aplicación es muy interactiva y se puede utilizar muy fácilmente.

- Configuración de la red a analizar

Posteriormente se realiza la configuración de los equipos para que exista comunicación con los servidores y conectadas tengan acceso a los servicios web informativos, la configuración que se realizó se puede observar en el Anexo H, en donde las direcciones IP utilizadas no son las verdaderas por motivos de que el DTIC no facilito dicha información por motivos de sus políticas de seguridad.

## 2.3. Identificación de las vulnerabilidades

Para la identificación de vulnerabilidades se utilizó la aplicación OWASP ZAP por motivos de que en el estudio anteriormente realizado como se puede observar en la tabla 1-5 es el segundo más efectivo, pero a diferencia OWASP ZAP es de licenciamiento libre, es decir se tiene la facilidad de utilizar la aplicación sin la realización de algún pago a diferencia de Acunetix tiene un valor desde los $ 6 995.

Para realizar el análisis de vulnerabilidades en OWASP ZAP se abre la aplicación que viene instalado por defecto en Kali Linux, la interfaz del analizador se puede observar en la figura 7-2.

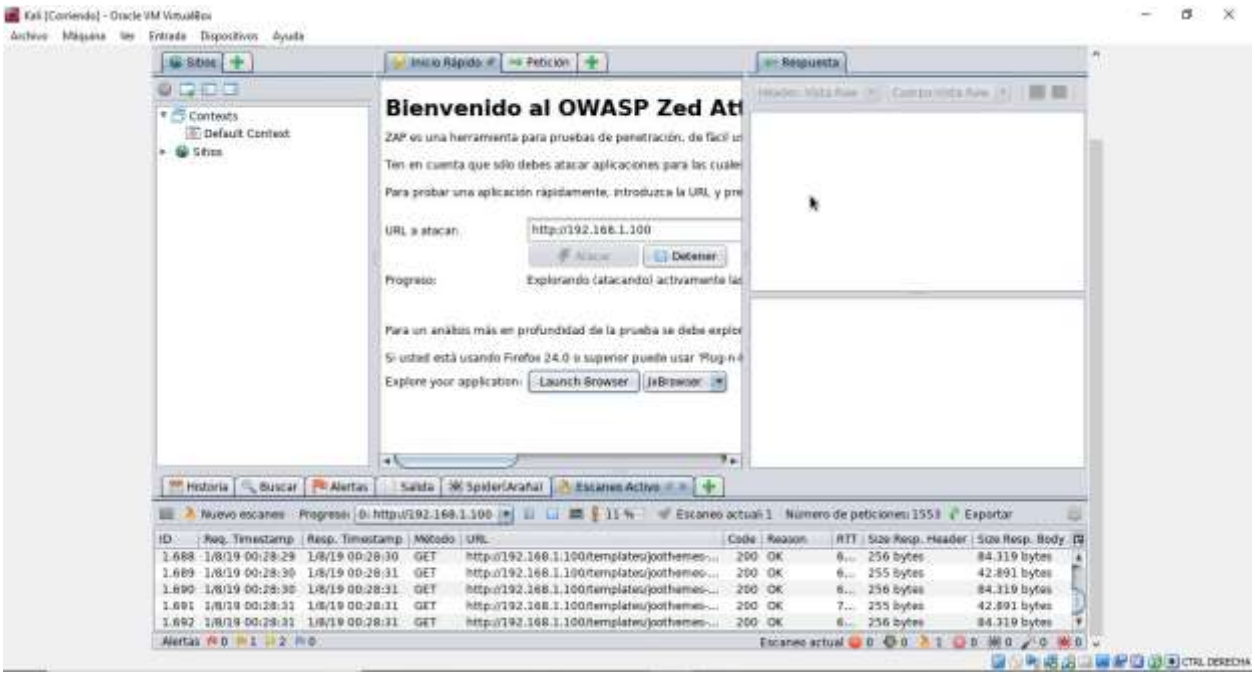



**Figura 7-2:** Interfaz de OWASP ZAP

**Realizado por:** Arias, Angel; 2019.

En la Figura 7-2 se puede observar la interfaz de OWASP ZAP en donde para la utilización se escribe la dirección IP de la página o servidor a analizar en el presente caso se analizó el servidor simulado del sistema web institucional informativo, posteriormente se da clic en Atacar y el analizador empezara a realizar las pruebas para entregar las vulnerabilidades que presente el servicio web informativo.

Al finalizar las pruebas la aplicación permite la realización de exportar un archivo en donde se encuentran todas las vulnerabilidades, donde el analizador tiene en cuenta el top ten de vulnerabilidades de OWASP, definiendo así la vulnerabilidad que se decide explotar siendo la denegación de servicio dado que es una de las más comunes y en los servicios web informativos lo más importante es que el usuario tenga acceso a la página siempre que desee utilizarla priorizando la disponibilidad.

## 2.4. Explotación de las vulnerabilidades

En el presente trabajo de titulación la vulnerabilidad que se explotó es la de denegación de servicio porque en los servicios web informativos la vulnerabilidad más común es respecto a la disponibilidad en donde se refiere que el usuario que desee informarse sobre lo que se encuentra publicado en el servicio web no tenga acceso. En la tabla 4-2 se puede observar el grado de nivel de dificultad de explotación, prevalencia, la detección y el impacto que tienen las vulnerabilidades. Teniendo en cuenta que cada uno de de los grados tiene su correspondiente ponderación de acuerdo a OWASP como se observa en la tabla 3-2:

**Tabla 3-2:** Niveles de amenaza de las vulnerabilidades.

| **Nivel de amenaza** | **Nivel explotación** | **Prevalencia de debilidades** | **Detección de debilidades** | **Impacto** |
|---|---|---|---|---|
| | Fácil (3) | Difundido (3) | Fácil (3) | Severo (3) |
| | Promedio (2) | Común (2) | Promedio (2) | Moderado (2) |
| | Difícil (1) | Poco común (1) | Dificíl (1) | Mínimo (1) |

**Fuente:** OWASP; 2017.

**Realizado por:** Arias, Angel; 2019.

**Tabla 4-2:** Ponderación de las diferentes vulnerabilidades.

| **Vulnerbilidad** | **Nivel explotación** | **Prevalencia** | **Detección** | **Impacto** |
|---|---|---|---|---|
| Inyección | 3 | 2 | 3 | 3 |
| Pérdida de autenticación | 3 | 2 | 2 | 3 |
| Exposición de datos sensibles | 2 | 3 | 2 | 3 |
| Entidades externas XML | 2 | 2 | 3 | 3 |
| Pérdida de acceso de control | 2 | 2 | 2 | 3 |
| Configuración de inseguridad incorrecta | 3 | 3 | 3 | 2 |
| Secuencia de comandos en sitios cruzados (XSS) | 3 | 3 | 3 | 2 |
| Deserelizacón insegura | 1 | 2 | 2 | 3 |
| Componentes con vulnerabilidades conocidas | 2 | 3 | 2 | 2 |
| Registro y monitoreo insuficientes | 2 | 3 | 1 | 2 |

| | | | | |
|---|---|---|---|---|
| Denegación de servicio | 3 | 2 | 3 | 3 |

**Fuente:** OWASP; 2017.

**Realizado por:** Arias, Angel; 2019.

Teniendo en cuenta la Tabla 4-2 y sabiendo que se el presente trabajo de titulación es destinado a los servicios web informativos, en el cual no se utilizan base de datos, contraseñas, entre otros datos, lo que interesa al DTIC es determinar la vulnerabilidad que tienen sus servicios web informativos y que siempre se encuentren disponibles para las personas que deseen utilizarlos, teniendo en cuenta estos aspectos, se realizaron dos tipos diferentes de ataque de denegación de SYN los cuales son:

- Ataque DDOS SYN con slowloris
- Ataque DDOS SYN con Metasploit

En donde se realizaron los dos ataques con los mismos parámetros para comparar los tiempos de denegación de servicio y el tiempo de recuperación del servicio web informativo cuando se detiene el ataque.

Para la realización del primer ataque se observa los códigos para la instalación y ejecución se observan en el Anexo K, las pruebas se realizaron en los tres servidores de medicina, DTIC y sistema web académico.

Para la realización de las pruebas en los tres diferentes servidores se realizó cada servidor por separado para tener más recursos en cada servidor y en la computadora atacante, las pruebas del ataque DDOS SYN con slowloris se utilizaron la cantidad de paquetes registrados por el grupo de investigación denominado "Propuesta de Solución SDN – Sistema de Aprendizaje para identificación y clasificación de amenazas internas que mejoren el control y la seguridad en intranets académicas.", en donde se tomó el tiempo de 1 segundo en todas las pruebas.

## 2.5. Comprobación de la explotación de las vulnerabilidades

Se realizó 30 pruebas para poder analizar con cada uno de los diferentes ataques DDOS SYN estadísticamente y en los tres diferentes servidores que contienen los servicios web informativos, se recopilaron los tiempos tanto de denegación como de recuperación como se puede observar en el Anexo M y con esos datos realizar las pruebas estadísticas T-student la cual permite ver cuál de los dos ataques DDOS SYN es más efectivo, es decir, cuál de los dos realiza la misma acción, pero en el menor tiempo. Para ello se tienen los mismos parámetros en todas las pruebas realizadas, es decir, el

tiempo será de 1 segundo en todas las pruebas y se atacará al puerto 80, el valor que cambiará en todos los ataques será los paquetes enviados basándose en el Anexo K.

## 2.6. Implementación de mejoras para mitigación de vulnerabilidades

Para la implementación de la mitigación de los ataques DDOS SYN se basó en un estudio realizado previamente en la Universidad Politécnica de Madrid titulado "DISEÑO DE UN SISTEMA DE SEGURIDAD PARA UN SERVIDOR WEB APACHE." Realizada por Samuel Ortega Sancho el 11 de julio de 2018, en el cual se instaló mod_qos. En el presente trabajo de titulación se utilizó el mismo módulo, pero configurado de diferente forma como se puede observar en el Anexo N. Mod_qos permite la realización de filtros para las conexiones entrantes al servidor web y con ello poder mitigar los ataques. (Ortega, 2018, pp. 85-86)

Como se puede observar en el Anexo N se encuentra el script encargado de la mitigación del ataque DDOS SYN, en donde se controla que tenga un máximo de conexiones de 100000 IP diferentes, con solo 50 conexiones por cada IP, 256 conexiones TCP activas, desactivar el keep-alive cuando el 70% de las conexiones TCP están ocupadas, sabiendo que el keep-alive son la conexiones no terminadas que se mantienen hasta que el cliente o servidor interrumpe la conexión. Tambien con el script se controla el mínimo de velocidad para peticiones como para respuestas, negando a los clientes lentos que bloquean al servidor.

La configuración y aplicación del Anexo N se pueden observar en las figuras 8-2 y 9-2. El mismo procedimiento de instalación y ejecución se realizó para los tres diferentes servidores que contienen los tres diferentes servicios web informativos.

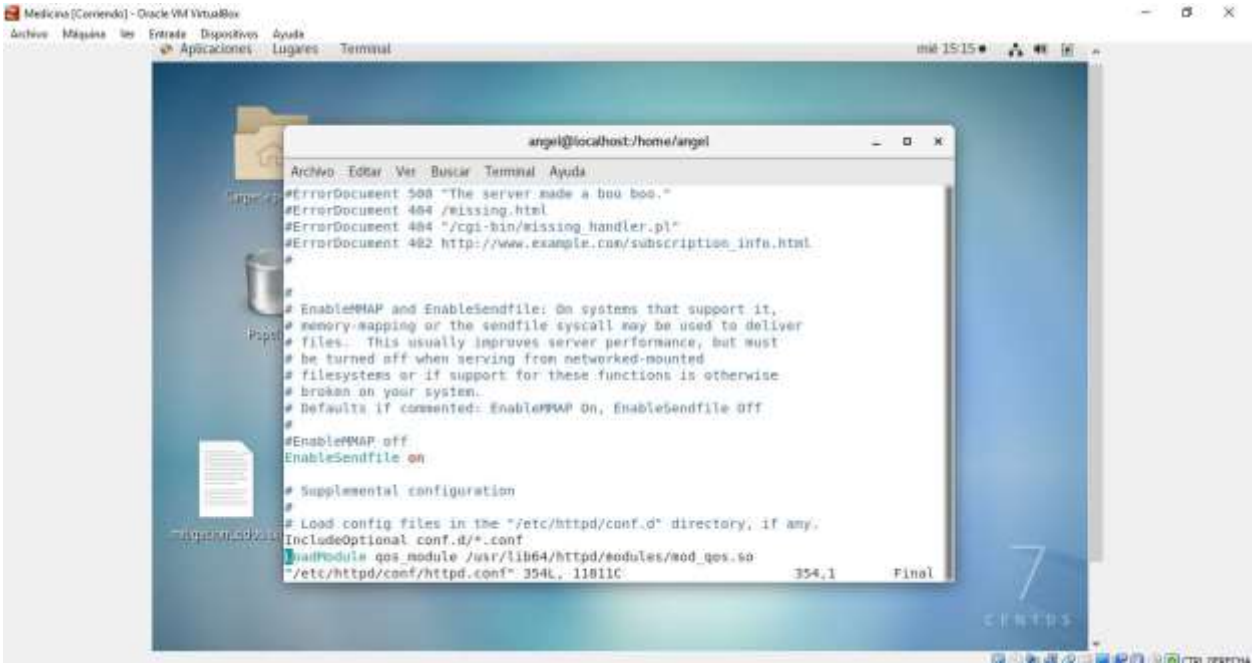



**Figura 8-2:** Configuración para que se ejecute el mod_qos.

**Realizado por:** Arias, Angel; 2019.

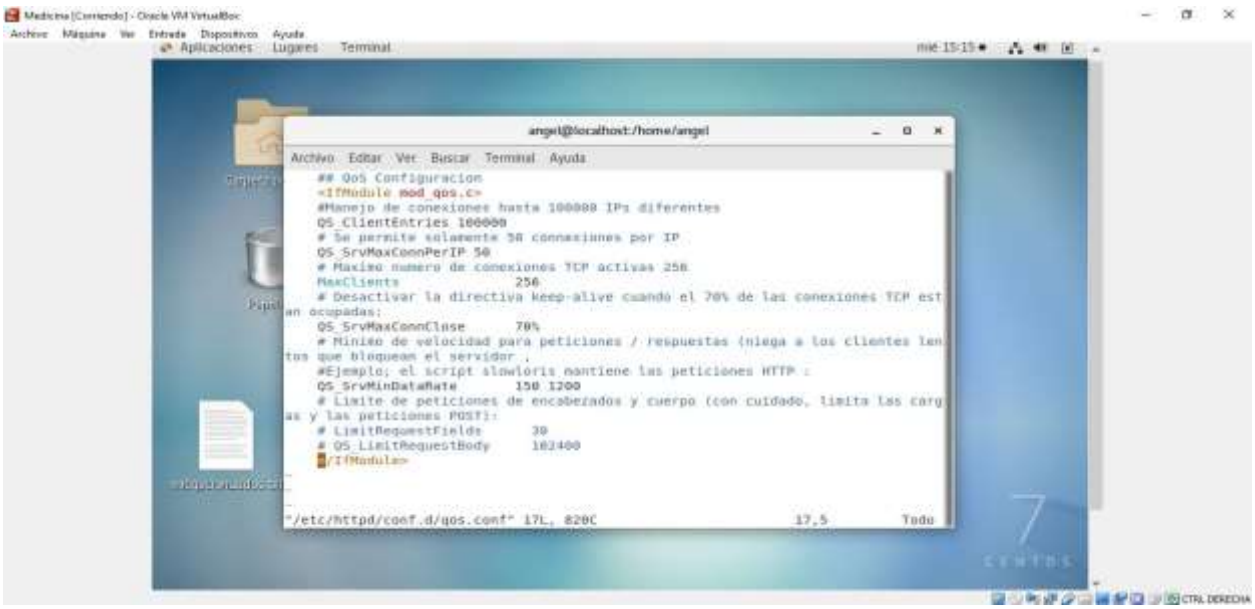



**Figura 9-2:** configuración para que funcione el mod_qos.

**Realizado por:** Arias, Angel; 2019.

## 2.7. Explotación y verificación de las vulnerabilidades corregidas

Una vez instalado el mod_qos, se procede a realizar las mismas 30 pruebas realizadas anteriormente para verificar que existe la mitigación de los ataques DDOS SYN, con la cantidad de paquetes que se encuentran en el Anexo K, en el cual igualmente se registró en este caso el tiempo de la carga del servicio web informativo tanto de medicina, DTIC y sistema web académico cuando se realizan los ataques DDOS SYN, se toma el tiempo desde que se empieza a realizar el ataque hasta que se carga el servicio por primera vez, dado que se realizó el ataque por varios minutos y nunca existió la denegación del servicio pero si se demoraba un cierto tiempo en cargar. Y a la vez se registró el tiempo que se demora en cargar el servicio desde que se detiene el ataque porque a diferencia de cuando se lo realizaba el tiempo de carga del servicio web informativo si varia.

# CAPÍTULO III

## 3. MARCO DE RESULTADOS Y DISCUSIÓN

En el presente trabajo de titulación se tuvieron los siguientes resultados:

### 3.1. Resultados de las encuestas realizadas

A continuación, se pueden observar los resultados que se obtuvieron para la recolección de información de la encuesta en el Anexo D.

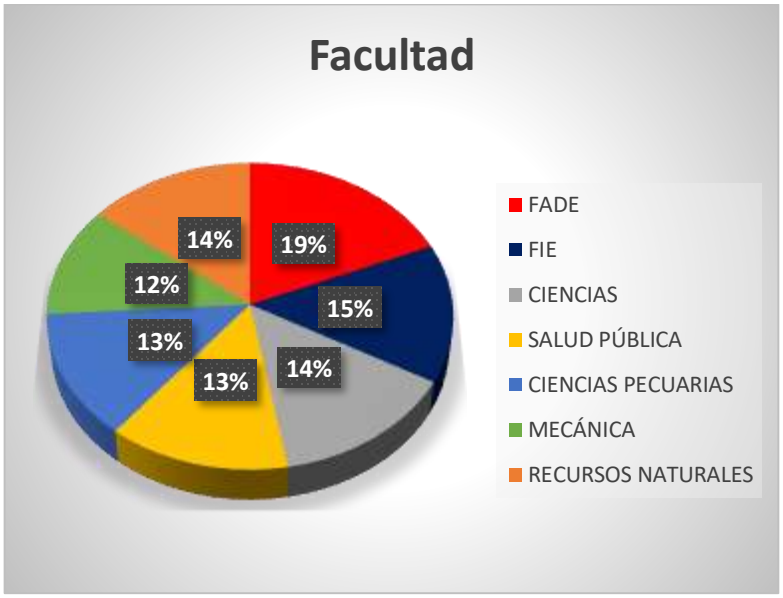



**Gráfico 1-3:** Porcentaje de estudiantes de cada facultad encuestados.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 1-3 se puede observar el porcentaje de los estudiantes de cada facultad que han sido encuestados de manera aleatoria, en el cual se tiene que un 19% de los estudiantes encuestados son de la Facultad de Administración de Empresas (FADE), el 15% son de la Facultad de Ingeniería Electrónica (FIE), el 14% equivale tanto a la Facultad de Ciencias como también a la Facultad de Recursos Naturales, el 13% corresponde a la Facultad de Ciencias Pecuarias como también a Salud Pública y el 12% corresponde a la Facultad de Mecánica.


**Gráfico 2-3:** Sistemas operativos más utilizados por los estudiantes de la ESPOCH.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 2-3 se puede observar que de todos los estudiantes que fueron encuestados los sistemas operativos más utilizados por los mismos son: Android con un 26%, Windows 10 con 25%, Windows 8 con 20%, Windows 7 con un 11% y finalmente Linux con un 11%. Lo cual nos quiere decir que, aunque el sistema operativo de Linux es el más seguro con relación a los demás es el menos utilizado ya puede ser por los conocimientos que se tienen del mismo sistema operativo.


**Gráfico 3-3:** Dispositivos más utilizados para utilizar los servicios web informativos de la ESPOCH.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 3-3 se puede observar que los estudiantes encuestados ingresan a los servicios web informativos de la ESPOCH utilizando más los siguientes dispositivos: celular, laptop, desktop (computadora de mesa) y Tablet con un porcentaje de utilización de: 35%, 32%, 18% y un 15% correspondientemente.

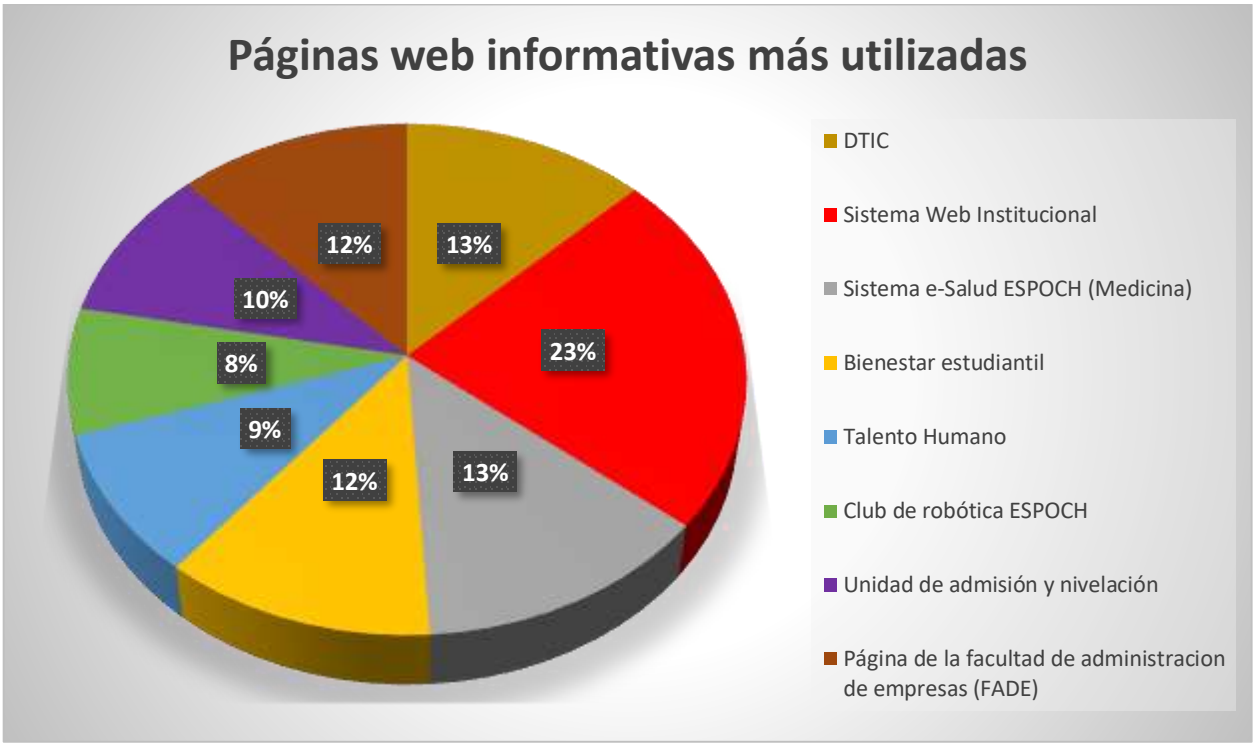



**Gráfico 4-3:** Páginas web informativas más utilizadas.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 4-3 se puede observar el porcentaje de los servicios web informativos más utilizados por los estudiantes de la ESPOCH, el cual sirve para poder tener los tres más utilizados para la simulación de los mismos. En el cual se tienen ocho servicios web informativos los cuales son:

- Sistema web institucional con un 23%.
- Sistema e-Salud ESPOCH (Medicina) con un 13%.
- DTIC con un 13%.
- Página de la FADE con un 12%.
- Bienestar Estudiantil con 12%.
- Página de la unidad de admisión y nivelación con un 10%.
- Página de talento humano con 9%.
- Y la página del club de robótica de la ESPOCH con un 8%.

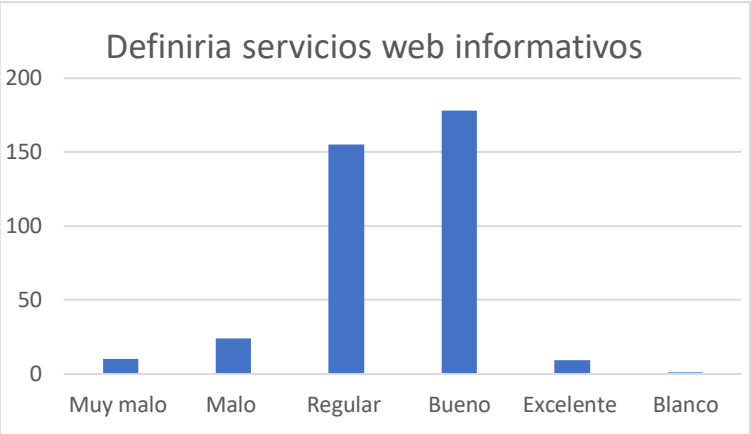



**Gráfico 5-3:** Calidad de los servicios web informativos de la ESPOCH.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 5-3 se puede observar un diagrama de barras en donde los estudiantes encuestados definieron la calidad que poseen los servicios web informativos, en donde, un estudiante no respondió y dejo en blanco, 9 estudiantes definieron al servicio como excelente, 178 estudiantes como bueno, 155 estudiantes como regular, 24 estudiantes lo definieron como malo y 10 estudiantes como muy malo.

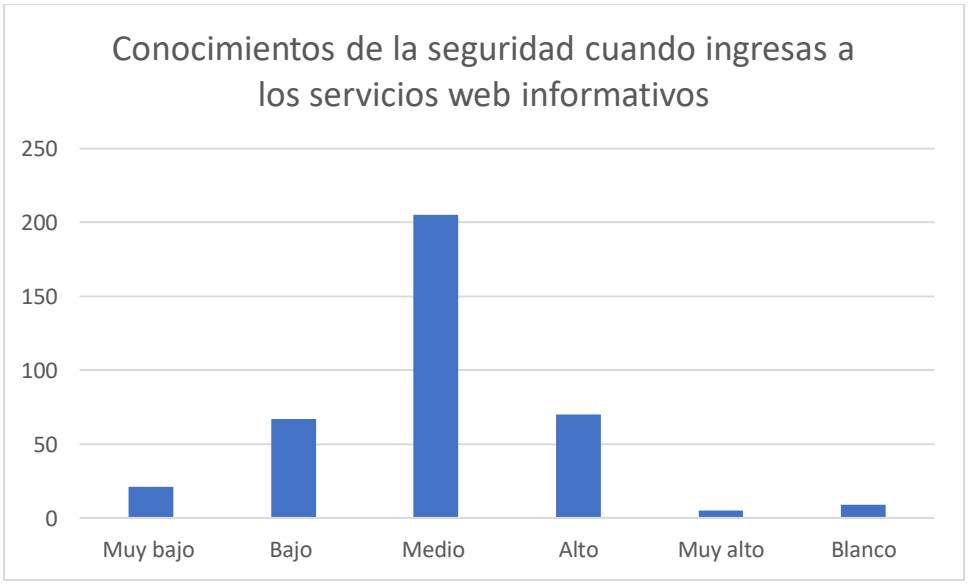



**Gráfico 6-3:** Conocimientos de seguridad cuando utilizan los servicios web informativos de la ESPOCH.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 6-3 se observa el grado de conocimientos que poseen los estudiantes acerca de la seguridad de los servicios web informativos en donde se puede observar que: 9 estudiantes dejaron en blanco la pregunta por desconocimiento sobre el tema, 5 estudiantes tienen un grado muy alto acerca de la seguridad de los servicios web informativos, 70 estudiantes tienen un nivel de conocimientos alto, 205 estudiantes tienen un grado de conocimiento de la seguridad de medio, 67 estudiantes poseen un grado de conocimiento bajo y 21 estudiantes poseen un grado muy bajo sobre la seguridad de los servicios web informativos de la ESPOCH.

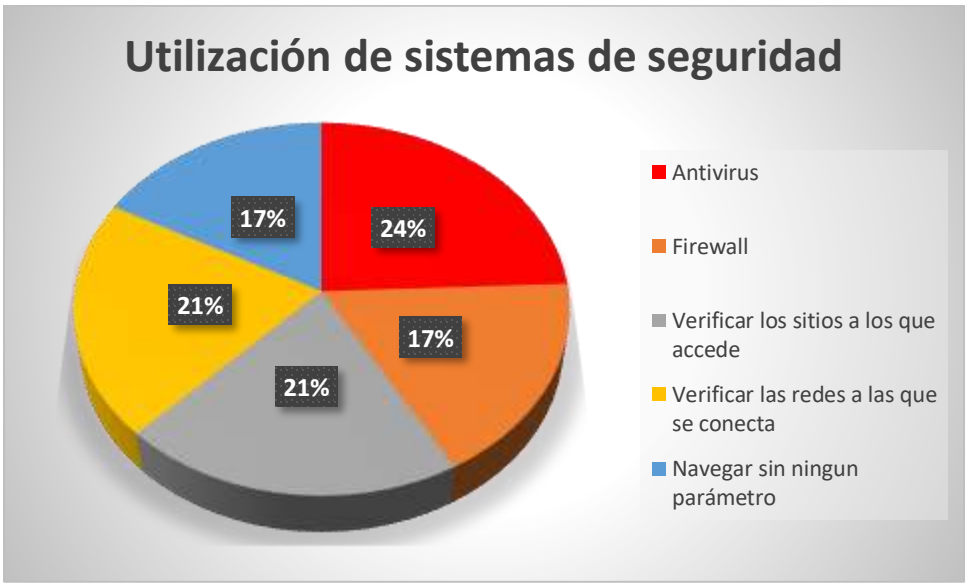



**Gráfico 7-3:** Porcentaje de utilización de sistemas de seguridad.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 7-3 se puede observar las protecciones con las que navegan cuando los estudiantes de la ESPOCH ingresan a los servicios web informativos, en donde, un 24% navega en el internet con la utilización de un antivirus, un 21% verifica las redes a las que se conectan, es decir, se conectan a redes conocidas, otro 21% verifica los sitios a los que acceden, el 17% utiliza firewall en el momento de navegar en internet y otro 17% navega sin tomar ningún parámetro de seguridad.

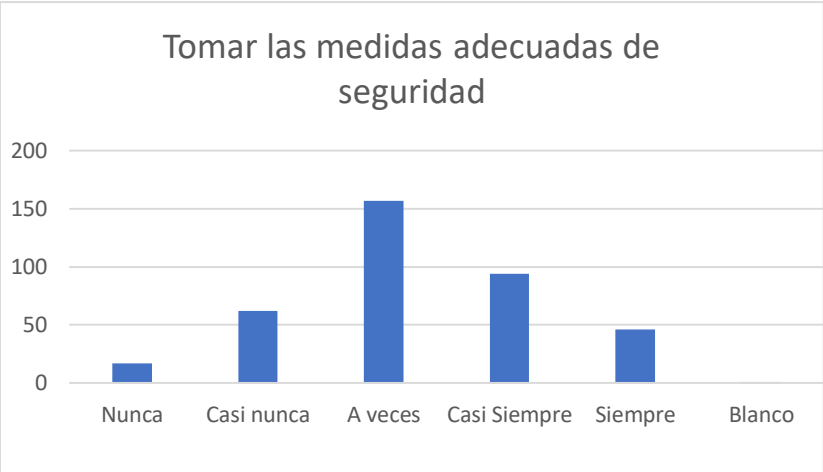



**Gráfico 8-3:** Medidas adecuadas que toman los estudiantes de la ESPOCH.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 8-3 se puede observar si los estudiantes toman medidas de seguridad cuando acceden a los servicios web informativos de la ESPOCH, en donde, 1 estudiante no respondió por desconocimiento, 46 respondieron que siempre, 94 respondieron casi siempre, 157 respondieron a veces, 62 respondieron casi nunca y 17 respondieron que nunca toman las medidas adecuadas de seguridad.

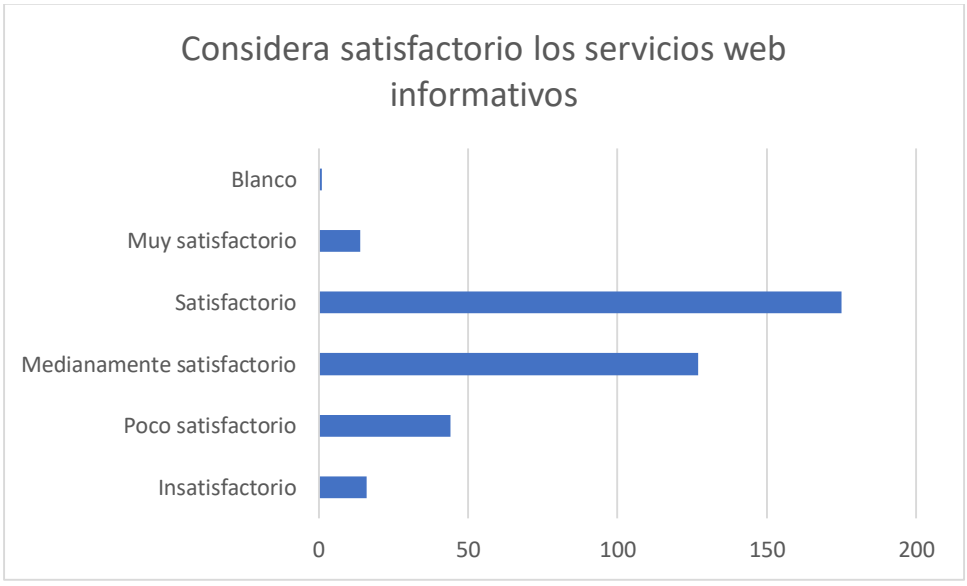



**Gráfico 9-3:** Nivel de satisfacción de los servicios web informativos de la ESPOCH.

**Realizado por:** Arias, Angel; 2019.

En la Gráfico 9-3 se observa como se sienten los estudiantes encuestados con los servicios web informativos de la ESPOCH, en donde, 1 estudiante no respondio, 14 estudiantes respondieron que

consideran muy satisfactorios los servicios web informativos, 175 consideran que son satisfactorios los servicios web informativos, 127 los consideran medianamente satisfactorios, 44 respondieron que son pocos satisfactorios y 16 estudiantes consideran insatisfactorios los servicios web informativos de la ESPOCH.

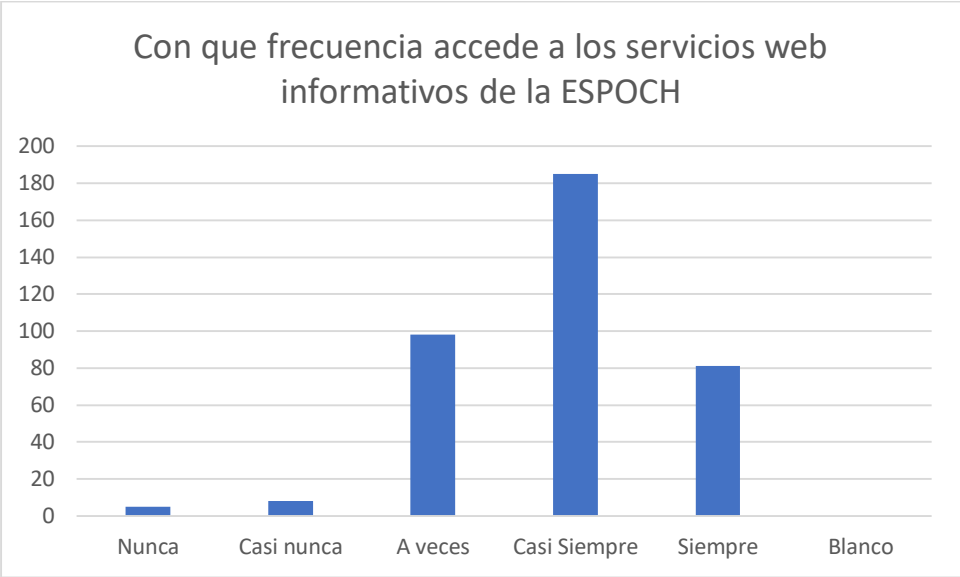



**Gráfico 10-3:** Frecuencia de utilización de los servicios web informativos de la ESPOCH.

**Realizado por:** Arias, Angel; 2019.

En la Gráfico 10-3 se puede observar la frecuencia con la que los estudiantes de la ESPOCH utilizan los diferentes servicios web informativos, en donde, 81 estudiantes respondieron que siempre utilizan los servicios web informativos, 185 estudiantes respondieron que utilizan casi siempre, 98 estudiantes que utilizan a veces, 8 que los utilizan casi nunca y 5 estudiantes respondieron que nunca utilizan los servicios web informativos, por lo cual se puede observar que es necesario tener con la menor cantidad de vulnerabilidades los mismos ya que son muy utilizados.

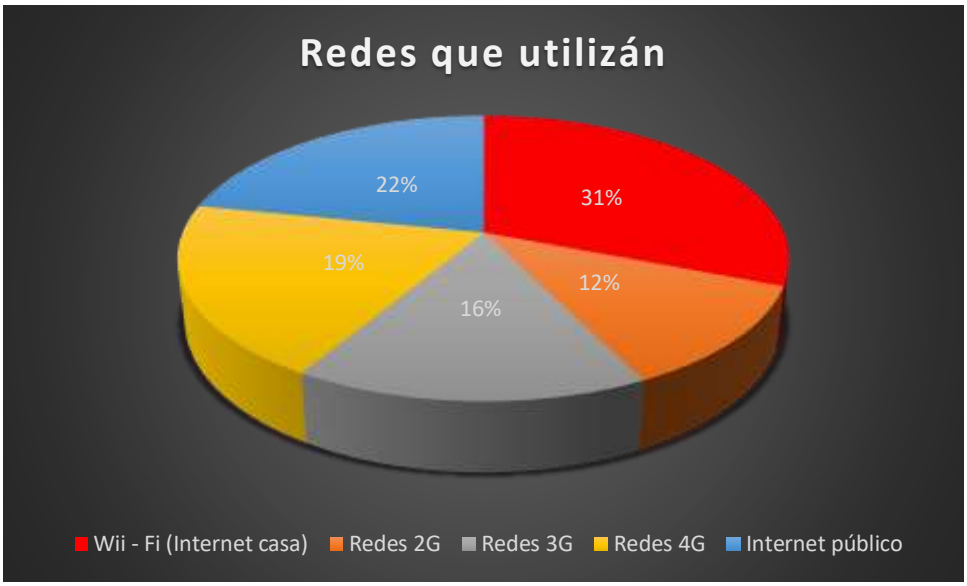



**Gráfico 11-3:** Redes que utilizan para utilizar los servicios web informativos de la ESPOCH.

**Realizado por:** Arias, Angel; 2019.

En la Gráfico 11-3 se puede observar las redes más utilizadas por los estudiantes para ingresar a los servicios web informativos de la ESPOCH, en donde, posee el porcentaje de 31%, 22%, 19%, 16% y 12% las redes WiFi (Internet de casa), internet público, redes 4G, redes 3G y las redes 2G respectivamente.

## 3.2. Instalación de los servicios web informativos

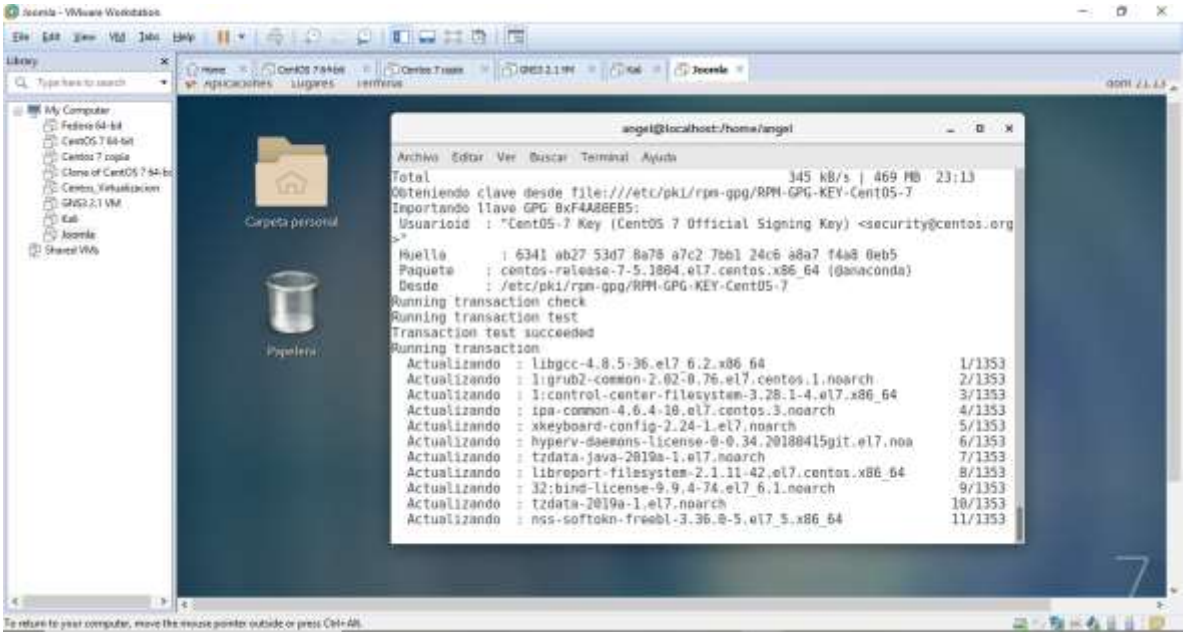



**Figura 1-3:** Actualización del sistema.

**Realizado por:** Arias, Angel; 2019.

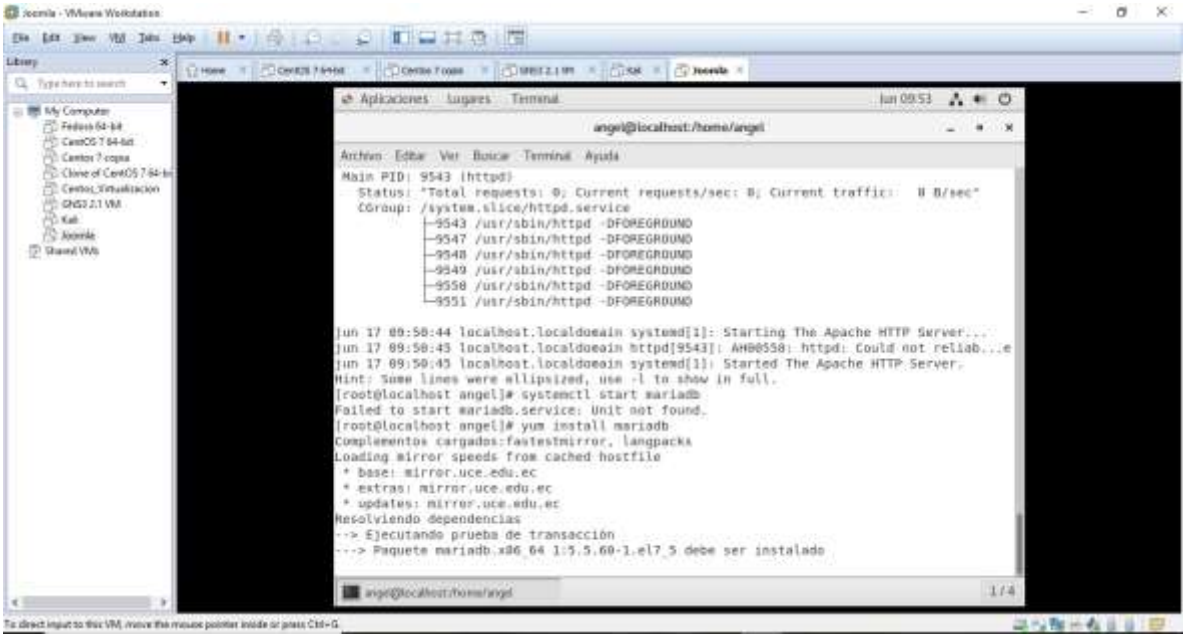



**Figura 2-3:** Instalación de mariadb.

**Realizapo por:** Arias, Angel; 2019.

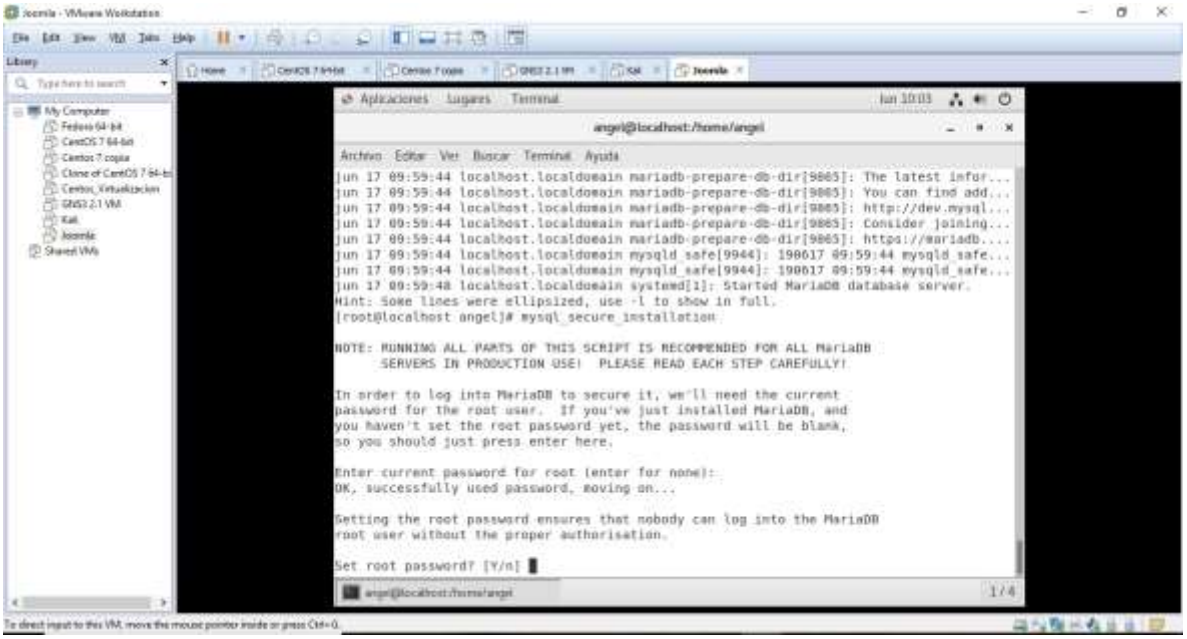



**Figura 3-3:** Instalación de mysql_secure.

**Realizado por:** Arias, Angel; 2019.

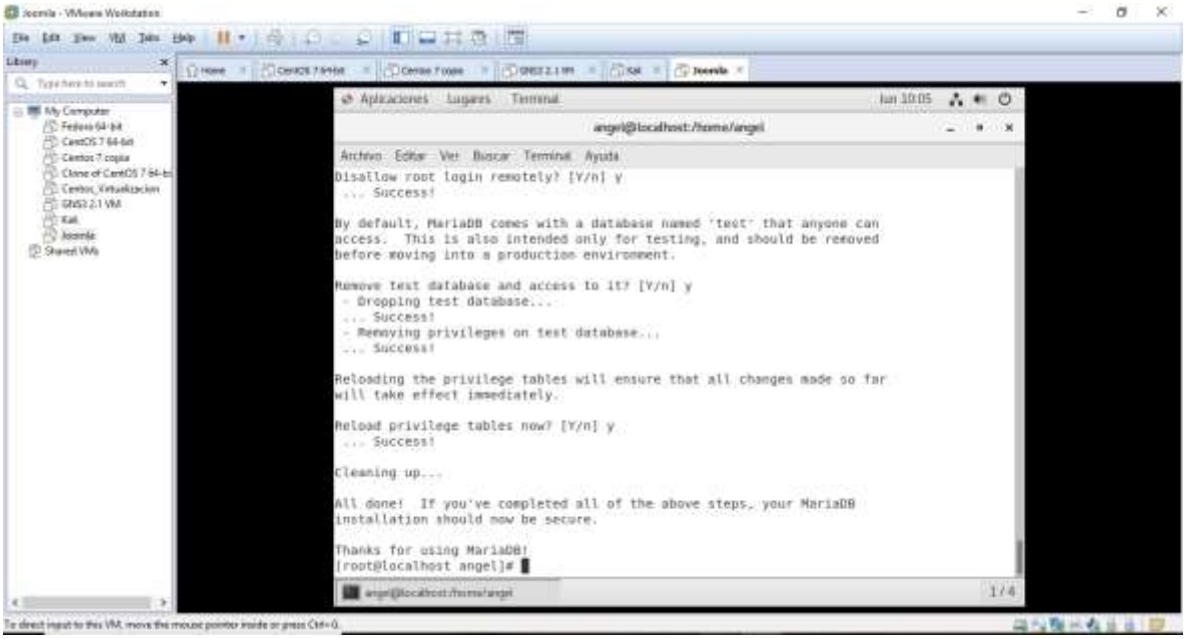



**Figura 4-3:** Opciones a elegir de mysql_secure.

**Realizado por:** Arias, Angel; 2019.

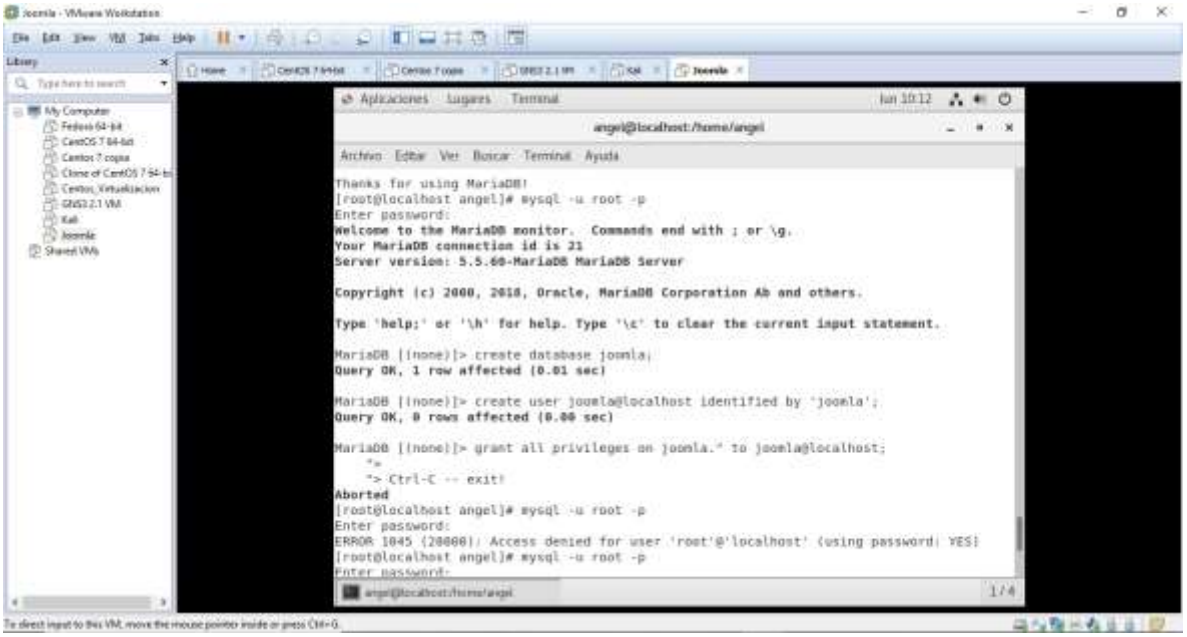



**Figura 5-3:** Configuración de joomla.

**Realizado por:** Arias, Angel; 2019.

En las Figuras 1-3 a la 5-3 se puede observar el proceso de instalación de joomla para la simulación de cada una de las páginas web informativas. Se utilizó joomla por motivos que en el momento de la recopilación de la información el DTIC informo que las páginas web informativas se encontraban en dicha plataforma, pero no especificaron las características de los servidores como la cantidad de memoria RAM entre otras características por motivos de políticas de seguridad.

Desde la figura 6-3 a la figura 8-3 se puede observar las direcciones IP de los tres diferentes servidores que contienen los servicios web informativos y desde la figura 9-3 a la figura 11-3 se observa que las computadoras tienen acceso a dichos servicios web informativos escribiendo en el navegador la dirección IP del servidor según sea el servicio al que se desea ingresar.

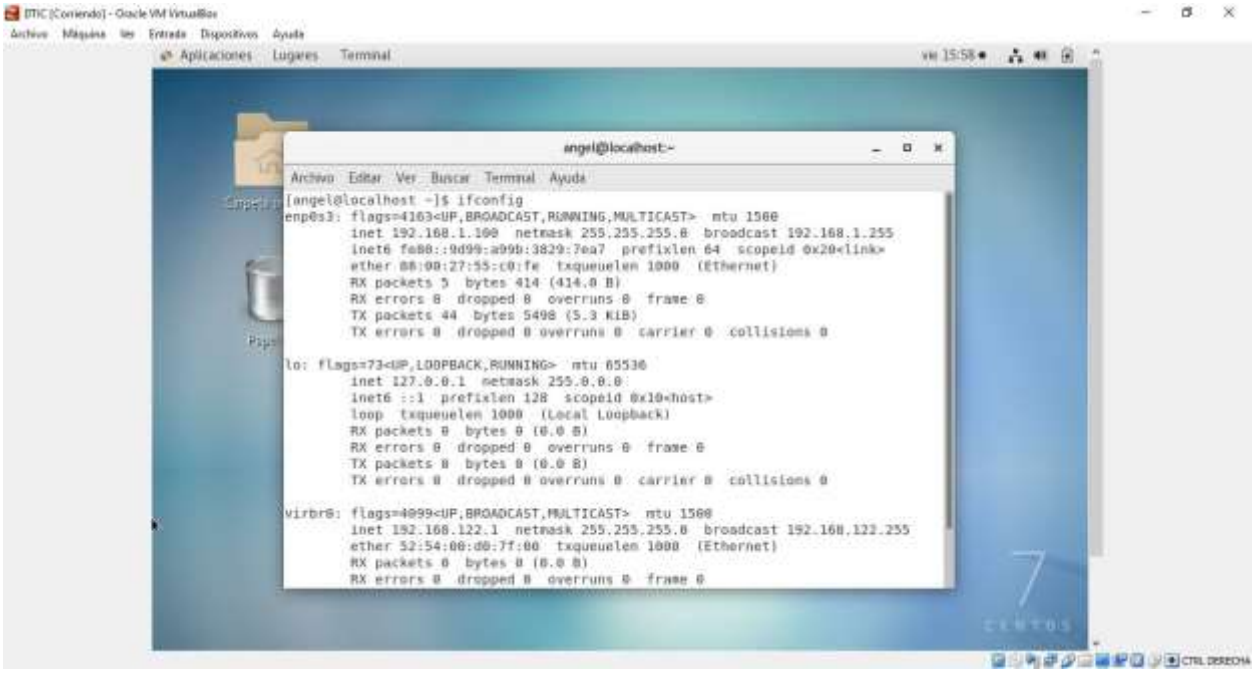



**Figura 6-3:** Dirección IP del servidor con el servicio web informativo del DTIC.

**Realizado por:** Arias, Angel; 2019.

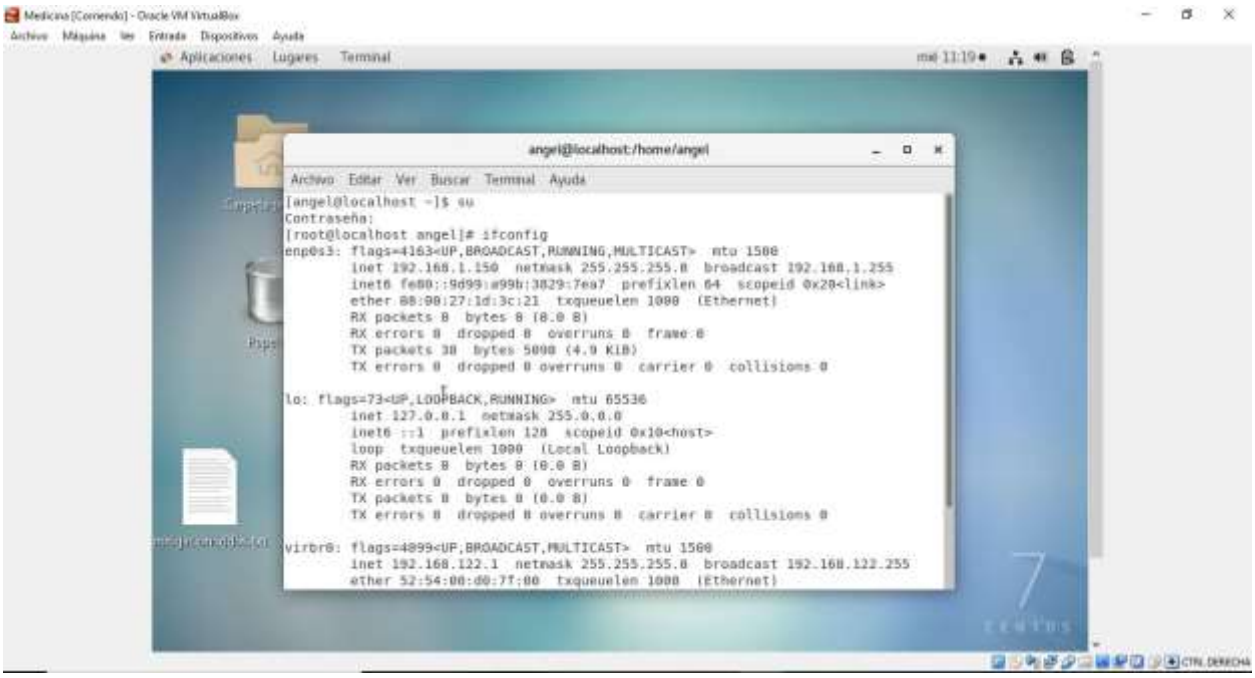



**Figura 7-3:** Dirección IP del servidor con el servicio web informativo de medicina.

**Realizado por:** Arias, Angel; 2019.

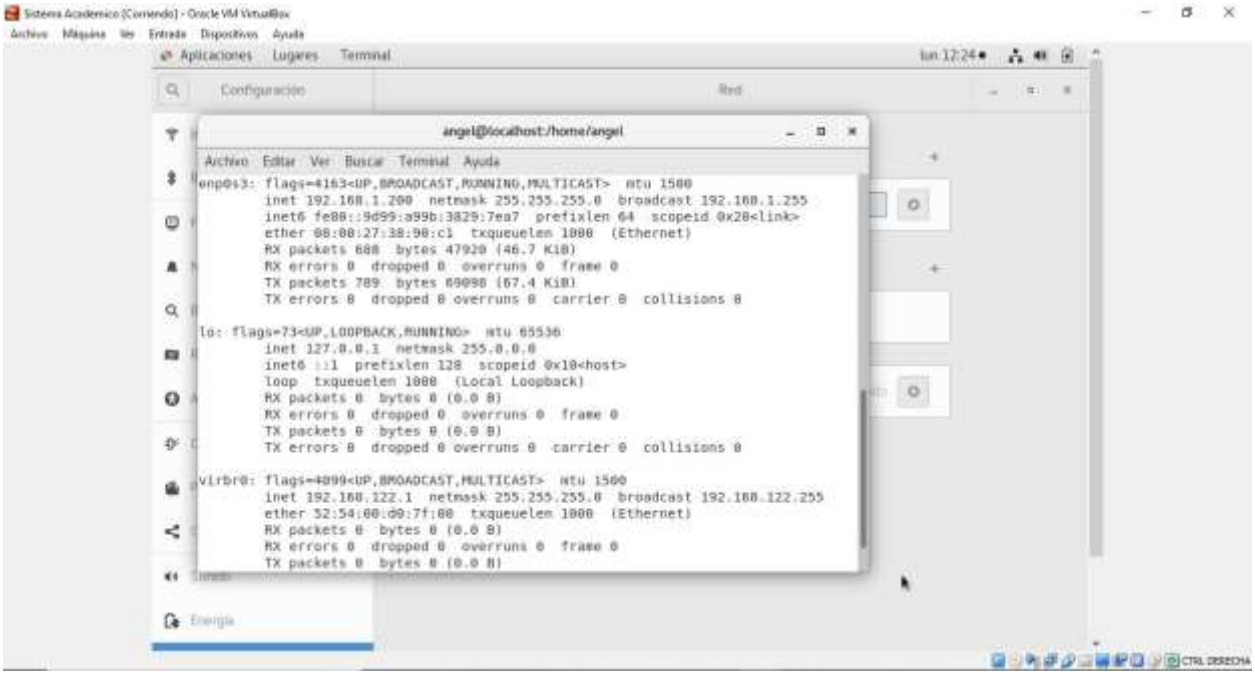



**Figura 8-3:** Dirección IP del servidor con el servicio web informativo del sistema académico.

**Realizado por:** Arias, Angel; 2019.

En las figuras de la 6-3 a 8-3 se puede observar las direcciones IP de los servidores que contienen los servicios web informativos del DTIC, medicina y sistema web académico respectivamente.

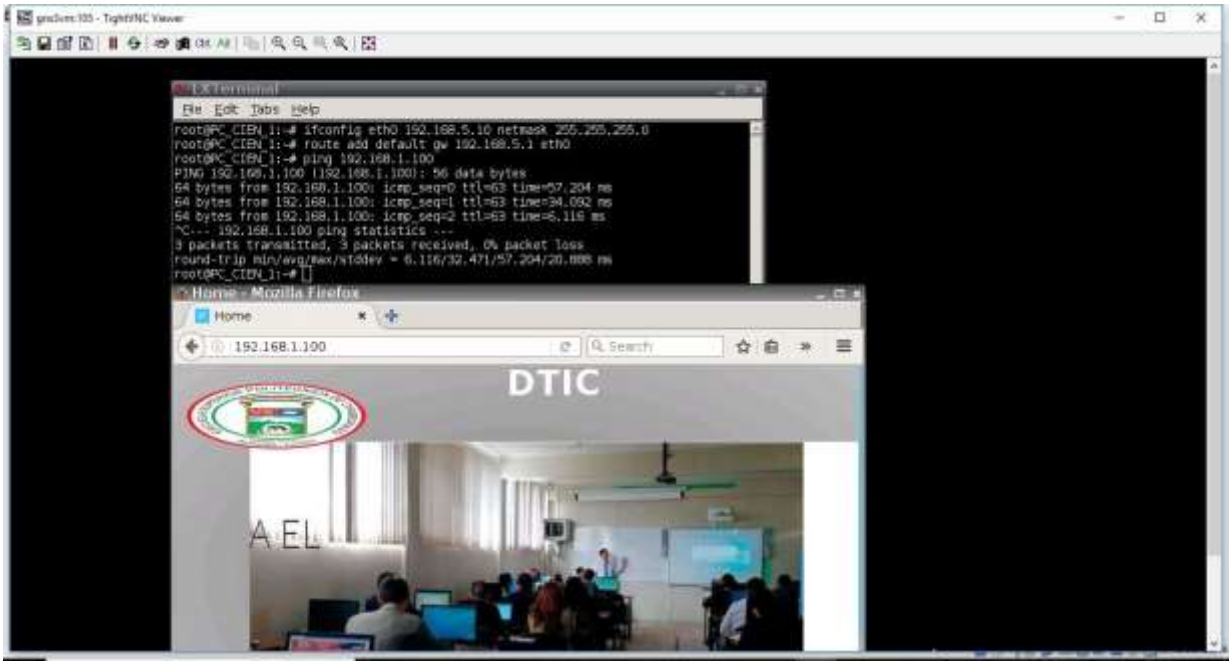



**Figura 9-3:** Acceso al servicio web informativo del DTIC.

**Realizado por:** Arias, Angel; 2019.

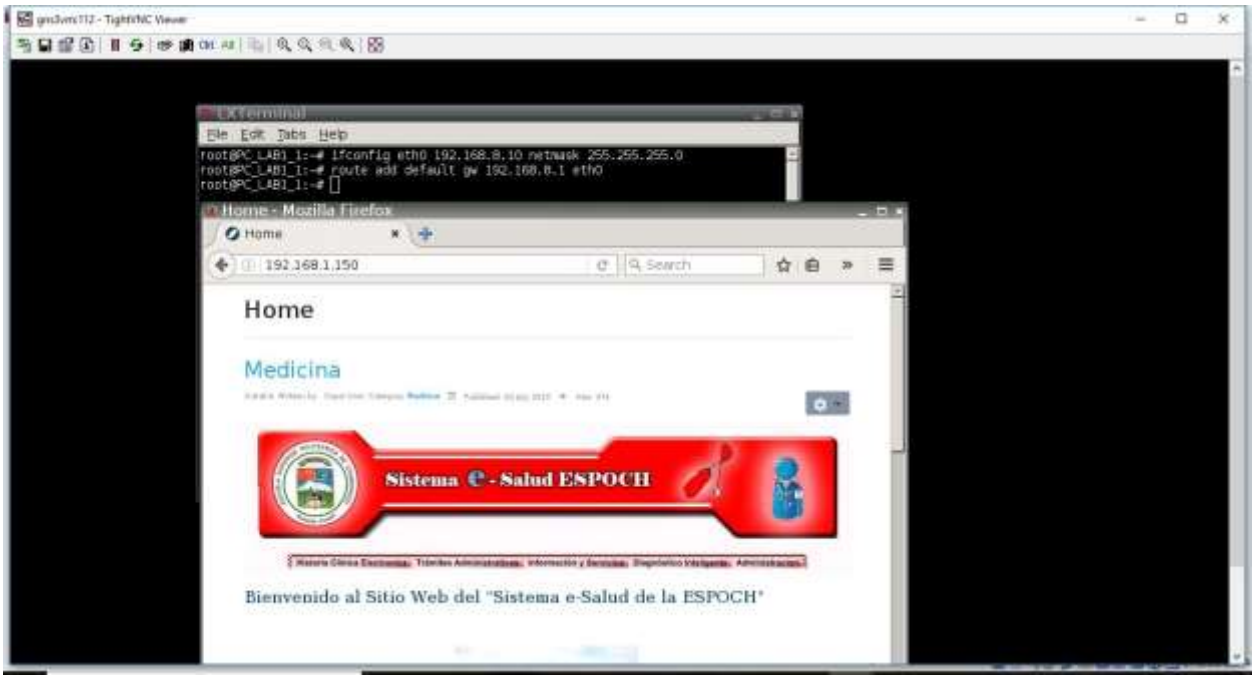



**Figura 10-3:** Acceso al servicio web informativo de medicina.

**Realizado por:** Arias, Angel; 2019.

c

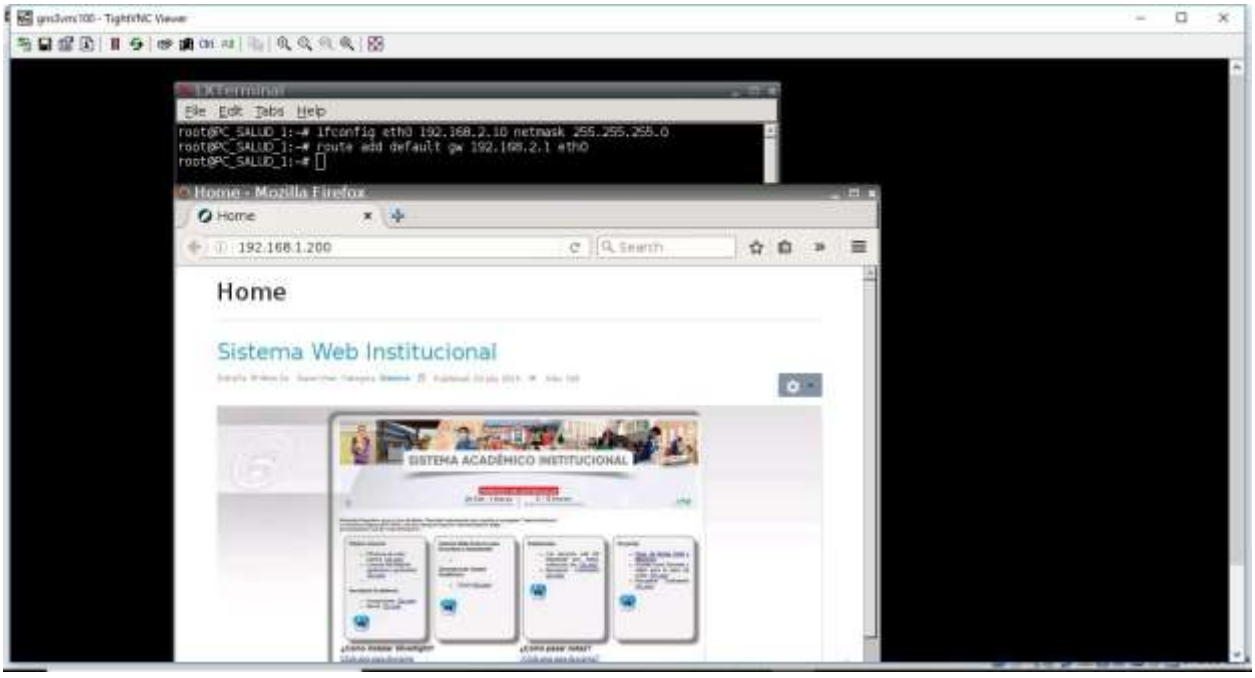



**Figura 11-3:** Acceso al servicio web informativo del sistema web institucional.

**Realizado por:** Arias, Angel; 2019.

Desde la figura 9-3 a la figura 11-3 se observa los servicios web informativos del DTIC, medicina y sistema web institucional funcionando en los cuales las computadoras en la red pueden acceder escribiendo 192.168.1.100, 192.168.1.150 y 192.168.1.200 que son las direcciones IP de los servidores correspondientemente.

### 3.3. Realización de Ataques DDOS SYN

En la figura 12-3 se observa la ejecución del ataque, el mismo ataque se realizó en los tres servidores que contenían los tres servicios web informativos distintos, pero con la cantidad de paquetes que se encuentran en el Anexo K.

En la figura 13-3 se observa que la prueba con el ataque fue exitosa y que se generó la denegación de servicio y los recursos de la computadora utilizada para la simulación durante la realización del ataque se observa en la figura 14-3, los tiempos de denegación como de recuperación del servicio se observan en las figuras 15-3 y 16-3 correspondientemente, dichos tiempos serán registrados para posteriormente comparar, comprobar e identificar cuál de los dos ataques de denegación de servicio fue más efectivo frente al otro ataque.

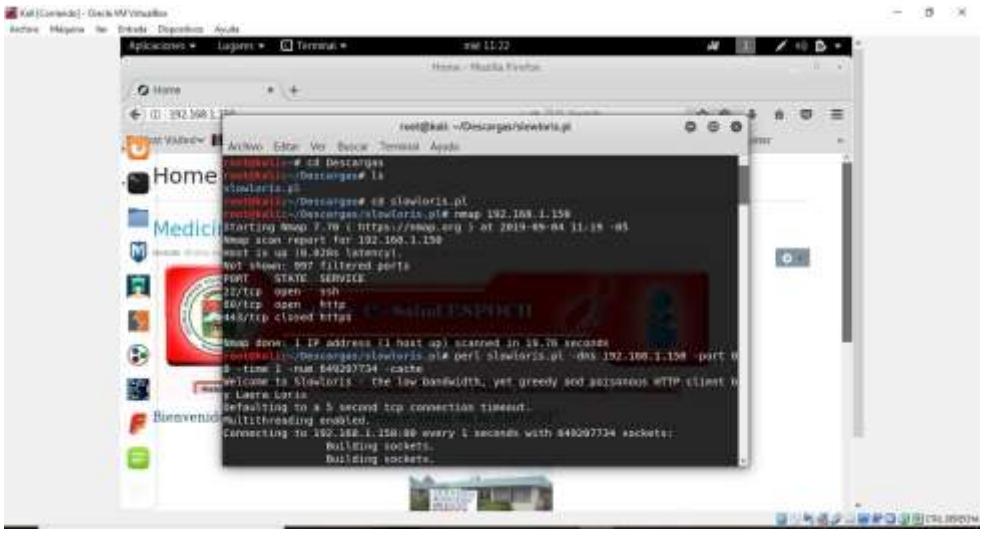



**Figura 12-3:** Ataque DDOS SYN con slowloris.

**Realizado por:** Arias, Angel; 2019.

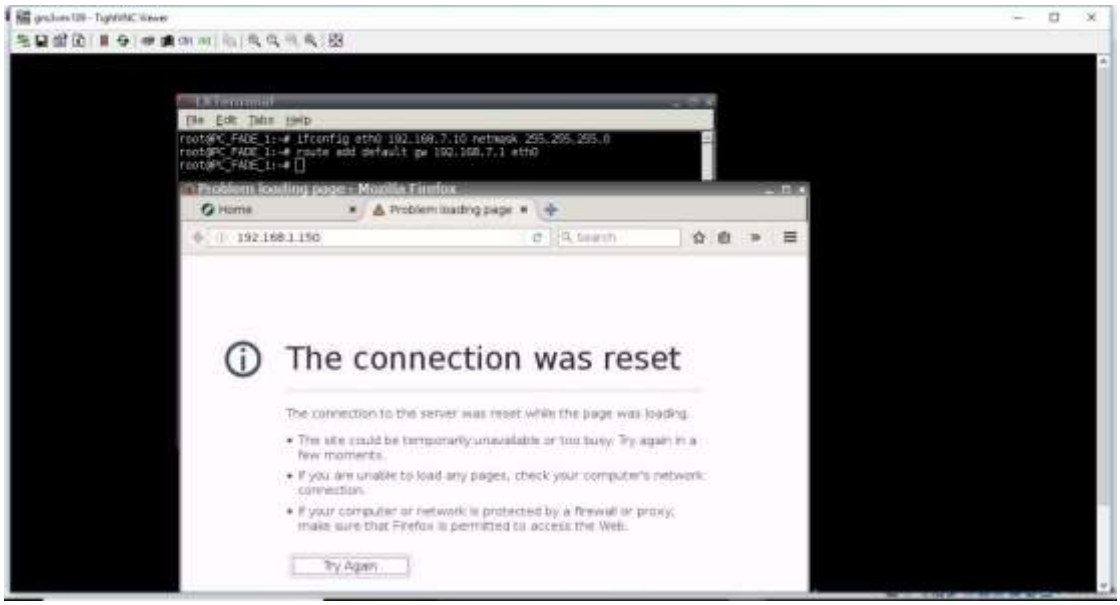



**Figura 13-3:** Comprobación del ataque DDOS SYN con slowloris.

**Realizado por:** Arias, Angel; 2019.

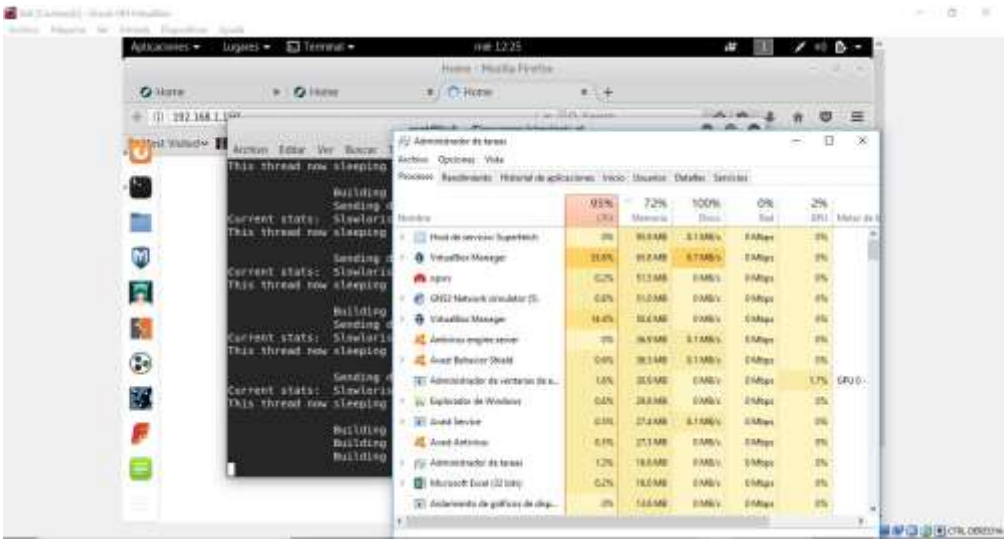


**Figura 14-3:** Recursos del computador durante el ataque DDOS SYN con slowloris.

**Realizado por:** Arias, Angel; 2019.

Desde la Figura 12-3 a la Figura 14-3 se puede observar que la realización y comprobación del ataque DDOS SYN con slowloris fue exitoso. El mismo procedimiento se realizó en los tres servidores que contienen los diferentes servicios web informativos, los parámetros son los mismos para poder comparar los diferentes tiempos posteriormente, lo que varía es la cantidad de paquetes que se utilizan lo cual se encuentra en el Anexo K.

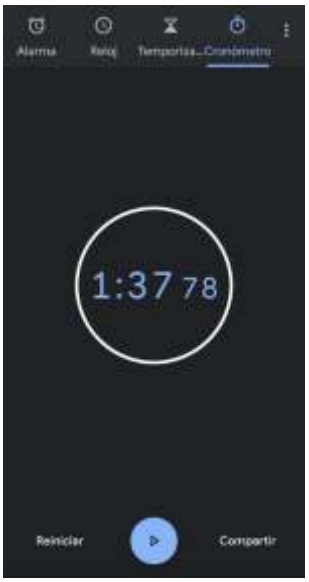



**Figura 15-3:** Tiempo de denegación del servicio del ataque DDOS SYN con slowloris.

**Realizado por:** Arias, Angel; 2019.

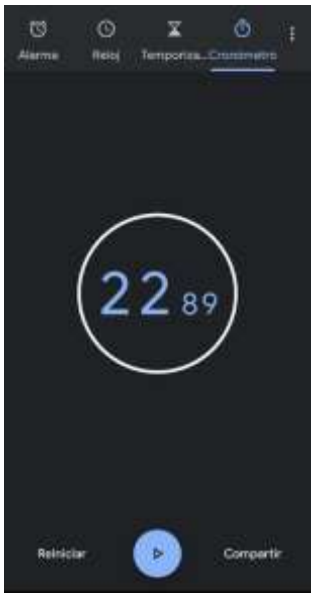



**Figura 16-3:** Tiempo de recarga del servicio del ataque DDOS SYN con slowloris.

**Realizado por:** Arias, Angel; 2019.

En la Figura 15-3 y 16-3 se observa los tiempos que se demora en realizar la denegación de servicio con slowloris y la recuperación del servicio web informativo después de que el ataque se finalizó correspondientemente, para lo cual se utilizó un cronometro para tomar los datos de las 30 pruebas

que se realizaron. El presente proceso de toma de tiempos se realizó para las pruebas tanto co slowloris como con Metasploit.

Para la realización de las pruebas con el segundo método se toman los mismos parámetros que son el tiempo de 1 segundo y la cantidad de paquetes que se encuentran en el Anexo K, la realización de las pruebas con el segundo método se puede observar desde la figura 17-3 a la figura 19-3, y los tiempos que se demora en realizar la denegacion y la recuperación del servicio web informativo en las figuras 20-3 y 21-3 correspondientemente. El presente procedimiento se lo realizo 30 veces, pero variando solo la cantidad de paquetes y los demás parámetros manteniéndolos iguales para poder compararlos posteriormente. el procedimiento para la realización del ataque con Metasploit se puede observar en el Anexo L.

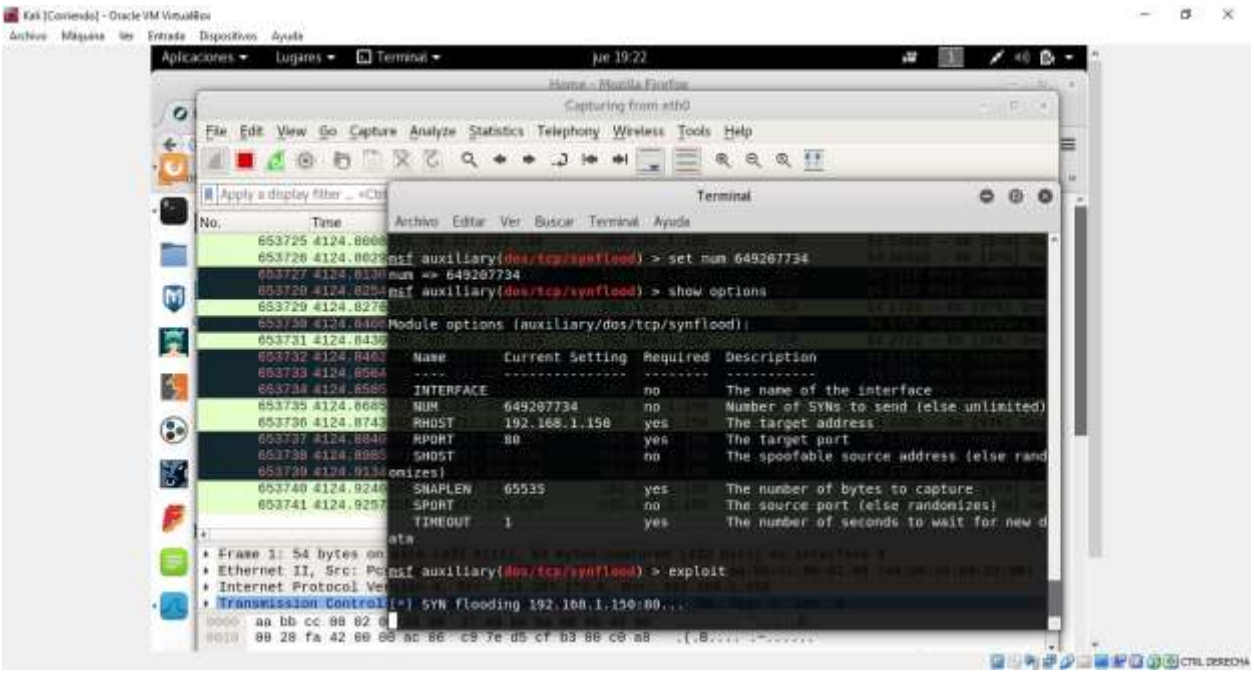



**Figura 17-3:** Ataque DDOS SYN con Metasploit.

**Realizado por:** Arias, Angel; 2019.

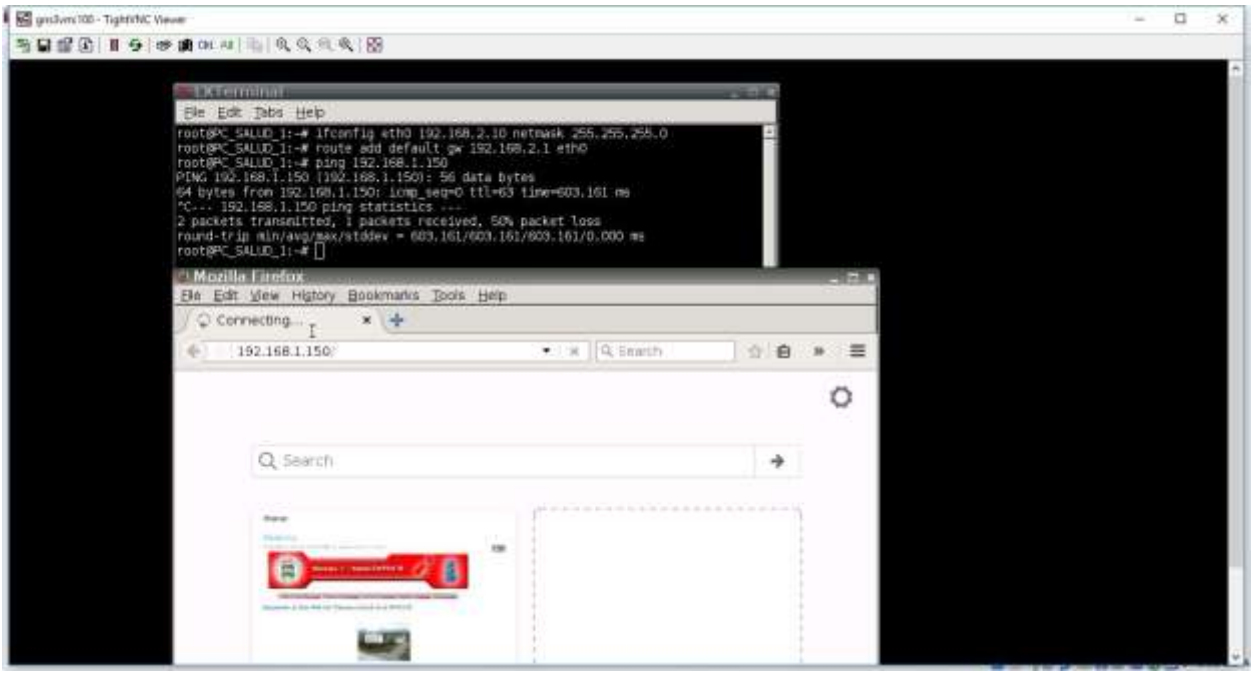



**Figura 18-3:** Comprobación del ataque DDOS SYN con Metasploit.

**Realizado por:** Arias, Angel; 2019

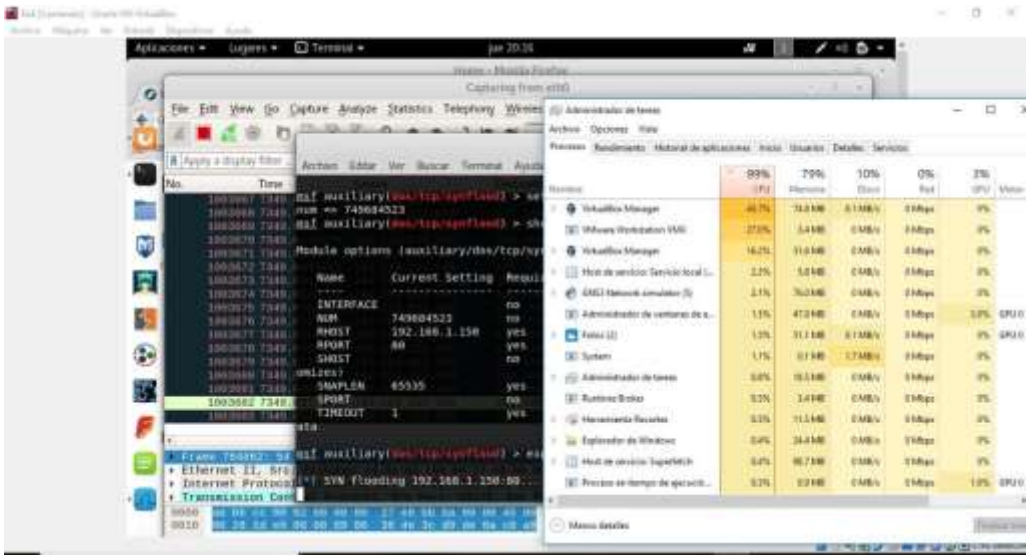


**Figura 19-3:** Recursos del computador durante el ataque DDOS SYN con Metasploit.

**Realizado por:** Arias, Angel; 2019.

Desde la Figura 17-3 a la Figura 18-3 se observa la realización del ataque DDOS SYN con Metasploit en donde lo principal que realiza es retardar la carga del servicio web informativo pero dicho proceso se realiza en un tiempo muy largo como se puede observar en la figura 20-3 y con ello los recursos

de donde se simula el escenario llega a utilizar demasiados recursos como se observa en la figura 19-3.


**Figura 20-3:** Tiempo de denegación del servicio del ataque DDOS SYN con Metasploit.

**Realizado por:** Arias, Angel; 2019.

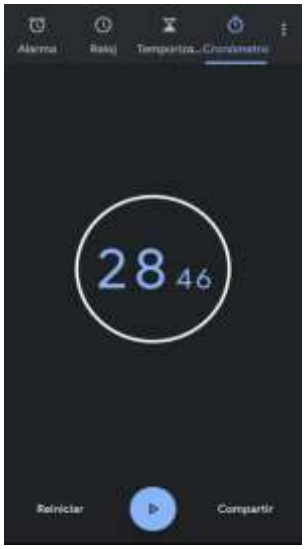



**Figura 21-3:** Tiempo de recarga del servicio del ataque DDOS SYN con slowloris.

**Realizado por:** Arias, Angel; 2019.

En la figura 20-3 y 21-3 se observa los tiempos que se demora para la realización del ataque DDOS SYN con Metasploit y el tiempo de recuperación del servicio cuando se finaliza el ataque correspondientemente, lo cual se realizó con un cronometro.

### 3.4. Pruebas T-student de los Ataques DDOS SYN

Los Gráficos realizados desde la 12-3 a la 17-3 se encuentran basados a los datos recopilados en el Anexo M mediante un cronómetro tanto para el tiempo de denegación del servicio web informativo como para el tiempo de recuperación del mismo, para la realización de la prueba T-student para la parte estadística se tomaron los mismos datos.

Teniendo en cuenta las figuras 12-3, 14-3 y 16-3 a la par que las tablas 1-3, 3-3 y 5-3 se puede observar que en todas las pruebas realizadas en los tres diferentes servidores que contienen los servicios web informativos de medicina, DTIC y sistema web académico, que el ataque DDOS SYN más efectivo es el realizado con slowloris ya que realiza la denegación en un tiempo mucho más rápido en los tres servicios analizados.

Analizando las figuras 13-3, 15-3 y 17-3 con las tablas 2-3, 4-3 y 6-3 se puede concluir que el tiempo de recuperación de los dos ataques DDOS SYN analizados en los tres servicios web informativos son muy parecidos, es decir, los tiempos de respuesta cuando se finalizan cualquiera de los dos ataques recargan relativamente al mismo tiempo, por lo tanto, si se desea realizar un ataque DDOS SYN se recomienda el ataque con slowloris ya que la denegación del servicio se realiza en un menor tiempo y la recuperación son parecidas en ambos ataques.

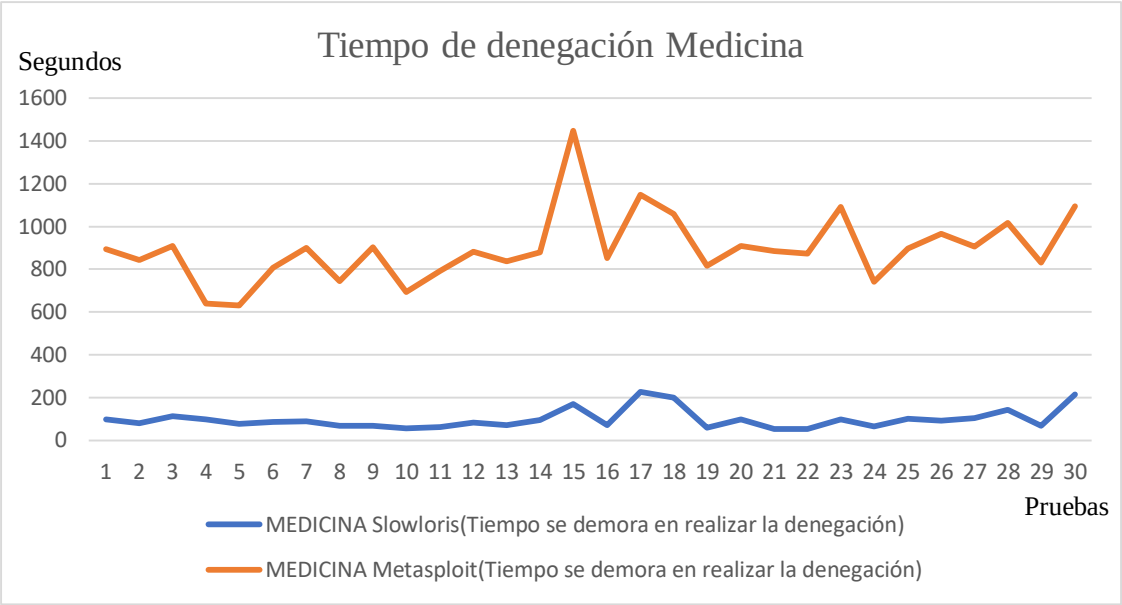



**Gráfico 12-3:** Tiempos de denegación en el servicio web informativo de medicina.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 12-3 se puede observar los resultados obtenidos de las pruebas realizadas en el servidor que contiene el servicio web informativo de medicina, en las que se tiene el tiempo que se demora cada uno de los dos diferentes ataques para que se realice la denegación del servicio.

**Tabla 1-3:** Prueba T-student con los tiempos de denegación de los ataques DDOS SYN en el servicio web de medicina.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 98.1683 | 668.3827 |
| Varianza | 2186.4410 | 26507.5843 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | 0.8454 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | -24.8299 | |
| P(T<=t) una cola | 2.1693E-21 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 4.3386E-21 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

En la tabla 1-3 se puede observar la prueba T-student para muestra de dos muestras emparejadas, en donde, los valores a tener en cuenta en primer lugar es P(T<=t) dos colas, lo que significa que la diferencia de medias son diferentes por lo tanto se acepta la hipótesis alternativa y con el dato estadístico t que es negativo, la hipótesis alternativa dice que el tiempo de respuesta del primer método es más rápido al tiempo de respuesta del segundo método, es decir, el ataque DDOS SYN con slowloris se realiza más rápido que el ataque DDOS SYN con Metasploit.

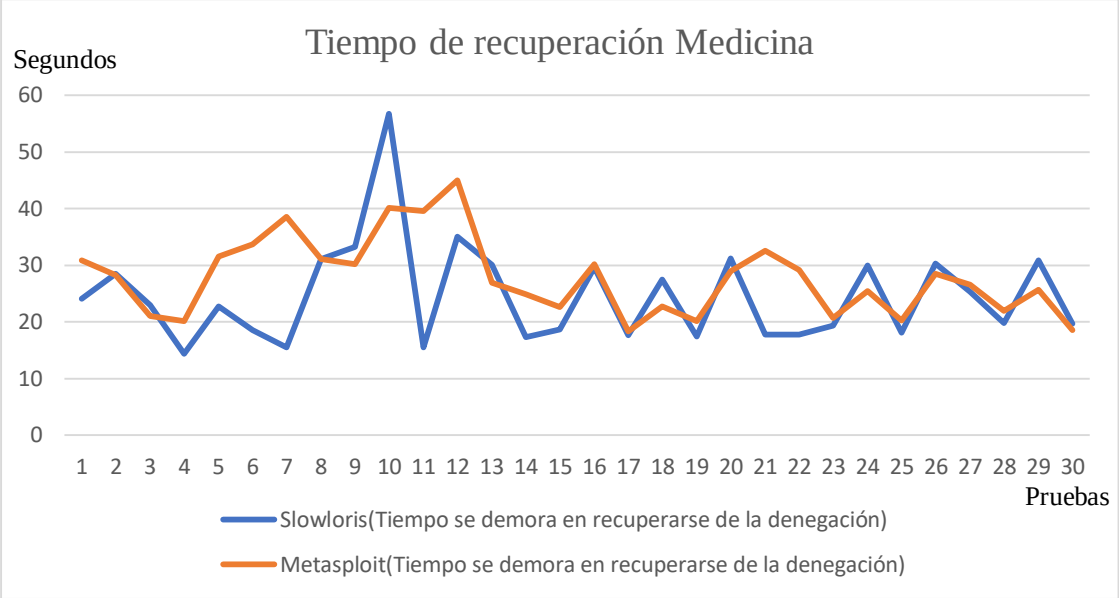



**Gráfico 13-3:** Tiempo de recuperación en el servicio web informativo de medicina.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 13-3 se observa el tiempo de recuperación del servicio web informativo de medicina, tanto para el ataque DDOS SYN con slowloris como con Metasploit, los tiempos registrados son desde que el ataque se finalice.

**Tabla 2-3:** Prueba T-student con los tiempos de recuperación de los ataques DDOS SYN al servicio web informativo de medicina.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 24.5460 | 27.7870 |
| Varianza | 75.6950 | 47.0616 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | 0.4221 | |
| Diferencia hipotética de las medias | 0.0000 | |

| | | |
|---|---|---|
| Grados de libertad | 29.0000 | |
| Estadístico t | -2.0868 | |
| P(T<=t) una cola | 0.0229 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 0.0458 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

En la tabla 2-3 se puede observar la prueba T-student para muestra de dos muestras emparejadas, en donde, los valores a tener en cuenta en primer lugar es P(T<=t) dos colas, lo que significa que la diferencia de medias redondeando son cero por lo tanto se acepta la hipótesis nula y con el dato estadístico t que es negativo, la hipótesis nula dice que el tiempo de respuesta del primer método es muy parecido al tiempo de respuesta del segundo método, es decir, el tiempo de recarga cuando se finaliza el ataque DDOS SYN con slowloris como con Metasploit es igual y no existe una diferencia significativa.

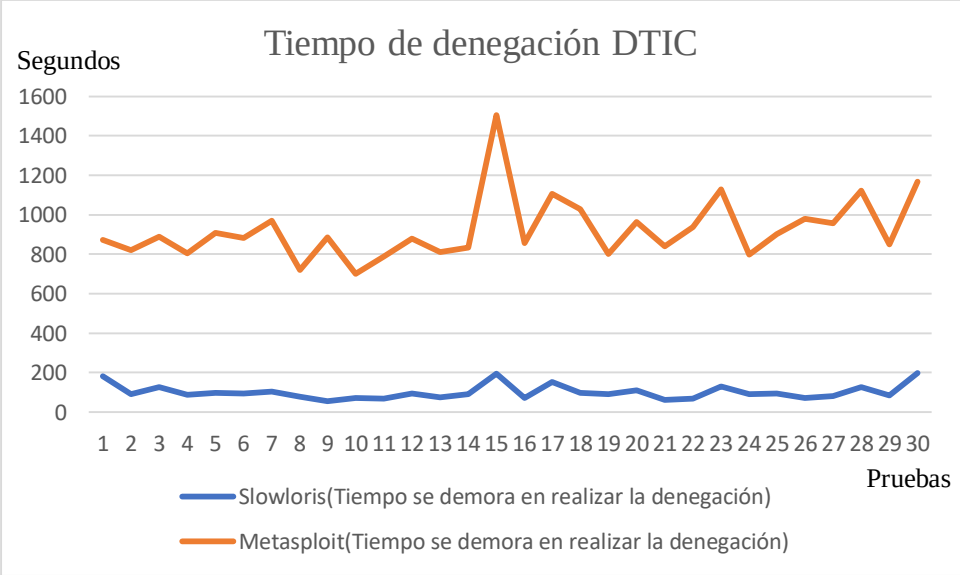



**Gráfico 14-3:** Tiempos de denegación en el servicio web informativo del DTIC.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 14-3 se puede observar los resultados obtenidos de las pruebas realizadas en el servidor que contiene el servicio web informativo del DTIC, en las que se tiene el tiempo que se demora cada uno de los dos diferentes ataques para que se realice la denegación del servicio.

**Tabla 3-3:** Prueba T-student con los tiempos de denegación de los ataques DDOS SYN en el servicio web del DTIC.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 101.8707 | 923.4917 |
| Varianza | 1393.2635 | 25568.4477 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | 0.7138 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | -33.1386 | |
| P(T<=t) una cola | 6.6406E-25 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 1.32812E-24 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

En la Tabla 3-3 se puede observar la prueba T-student para muestra de dos muestras emparejadas en el servicio web informativo del DTIC, en donde, el primer valor a analizar es P(T<=t) dos colas, lo que significa que la diferencia de medias son diferentes por lo tanto se acepta la hipótesis alternativa y con el dato estadístico t que es negativo, la hipótesis alternativa dice que el tiempo de respuesta del primer método es más rápido al tiempo de respuesta del segundo método, es decir, el ataque DDOS SYN con slowloris se realiza más rápido que el ataque DDOS SYN con Metasploit.

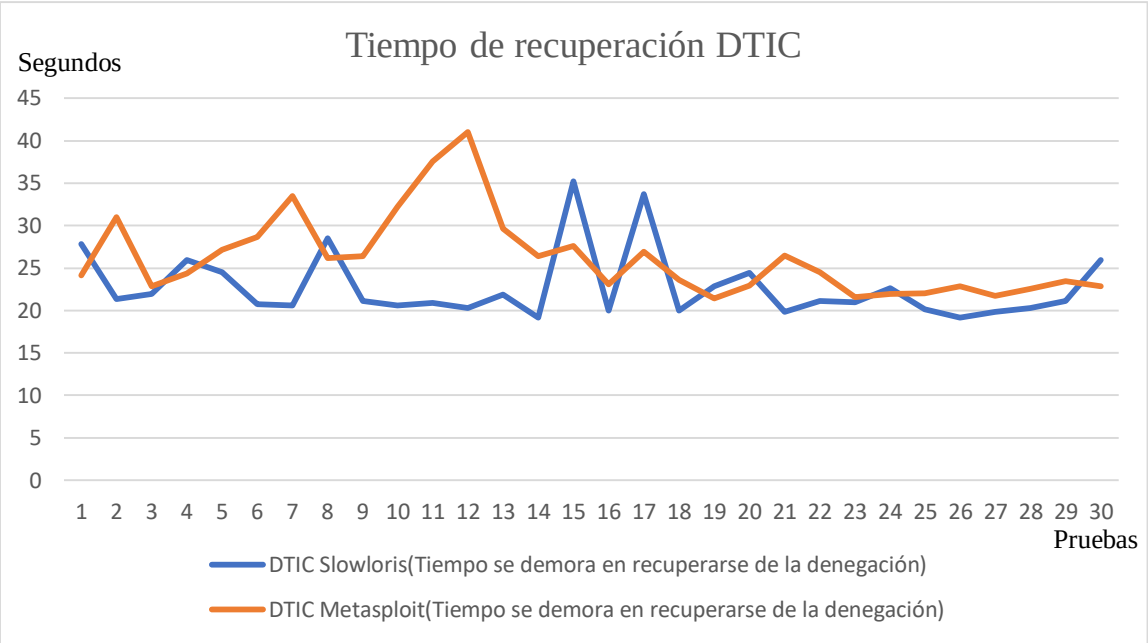



**Gráfico 15-3:** Tiempo de recuperación en el servicio web informativo del DTIC.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 15-3 se observa el tiempo de recuperación del servicio web informativo del DTIC, tanto para el ataque DDOS SYN con slowloris como con Metasploit, los tiempos registrados son desde que el ataque se finalice.

**Tabla 4-3:** Prueba T-student con los tiempos de recuperación de los ataques DDOS SYN al servicio web informativo del DTIC.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 22.7547 | 26.2217 |
| Varianza | 16.2401 | 23.2776 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | -0.0524 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | -2.9458 | |
| P(T<=t) una cola | 0.0031 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 0.0063 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

En la tabla 4-3 se tiene la prueba T-student para muestra de dos muestras emparejadas, en donde, el primer valor a analizar es P(T<=t) dos colas, lo que significa que la diferencia de medias redondeando son cero por lo tanto se acepta la hipótesis nula y con el dato estadístico t que es negativo, la hipótesis nula quiere decir que el tiempo de respuesta del primer método es muy parecido al tiempo de respuesta del segundo método, es decir, el tiempo de recarga cuando se finaliza el ataque DDOS SYN con slowloris como con Metasploit es igual y no existe una diferencia significativa.

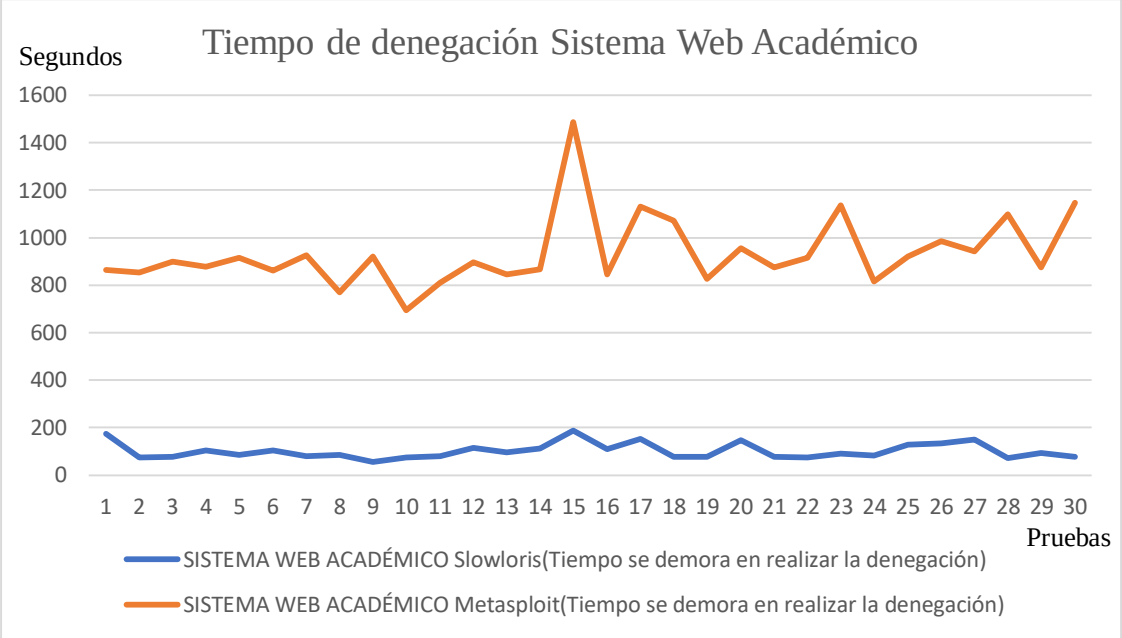



**Gráfico 16-3:** Tiempos de denegación en el servicio web informativo del Sistema Web Académico.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 16-3 se puede observar los resultados obtenidos de las pruebas realizadas en el servidor que contiene el servicio web informativo del Sistema Web Académico, en las que se tiene el tiempo que se demora cada uno de los dos diferentes ataques para que se realice la denegación del servicio.

**Tabla 5-3:** Prueba T-student con los tiempos de denegación de los ataques DDOS SYN en el servicio web del Sistema Web Académico.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 101.6017 | 934.2123 |
| Varianza | 1109.3156 | 22582.3836 |
| Observaciones | 30.0000 | 30.0000 |

| | | |
|---|---|---|
| Coeficiente de correlación de Pearson | 0.4138 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | -32.6163 | |
| P(T<=t) una cola | 1.04046E-24 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 2.08091E-24 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

En la tabla 5-3 se observa la prueba T-student para medias de dos muestras emparejadas en el servicio web informativo del Sistema Web Académico, en donde, el primer valor a analizar es P(T<=t) dos colas, lo que significa que la diferencia de medias son diferentes por lo tanto se acepta la hipótesis alternativa y con el dato estadístico t que es negativo, la hipótesis alternativa dice que el tiempo de respuesta del primer método es más rápido al tiempo de respuesta del segundo método, es decir, el ataque DDOS SYN con slowloris se realiza más rápido que el ataque DDOS SYN con Metasploit.

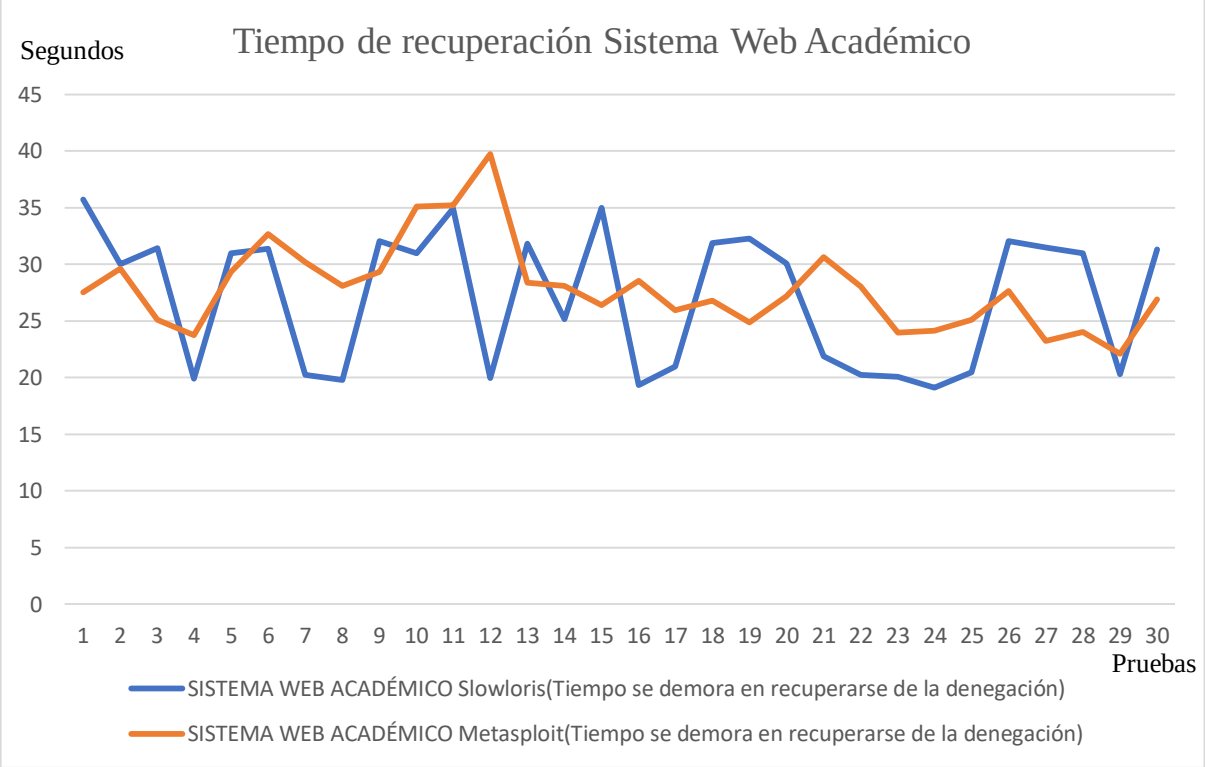



**Gráfico 17-3:** Tiempo de recuperación en el servicio web informativo del Sistema Web Académico.

**Realizado por:** Arias, Angel; 2019.

En el Gráfico 17-3 se observa el tiempo de recuperación del servicio web informativo del Sistema Web Académico, tanto para el ataque DDOS SYN con slowloris como con Metasploit, los tiempos registrados son desde que el ataque se finalice.

**Tabla 6-3:** Prueba T-student con los tiempos de recuperación de los ataques DDOS SYN al servicio web informativo del Sistema Web Académico.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 27.0593 | 27.9243 |
| Varianza | 35.7429 | 15.1687 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | 0.1038 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | -0.6980 | |
| P(T<=t) una cola | 0.2454 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 0.4908 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

En la tabla 6-3 se tiene la prueba T-student para muestra de dos muestras emparejadas para el servicio web informativo del Sistema Web Académico, en donde, el primer valor a analizar es P(T<=t) dos colas, lo que significa que la diferencia de medias redondeando son cero por lo tanto se acepta la hipótesis nula y con el dato estadístico t que es negativo, la hipótesis nula quiere decir que el tiempo de respuesta del primer método es muy parecido al tiempo de respuesta del segundo método, es decir, el tiempo de recarga cuando se finaliza el ataque DDOS SYN con slowloris como con Metasploit es igual y no existe una diferencia significativa.

### 3.5. Pruebas T-student de los Ataques DDOS SYN instalado mod_qos

En las Figuras 22-3 y 23-3 se puede observar la realización de los ataques DDOS SYN con slowloris y Metasploit respectivamente, el mismo procedimiento se realizó en cada uno de los tres servidores que contienen los tres servicios web informativos, y en ninguno de las pruebas realizadas se sufrió la

denegación del servicio, sufriendo máximo una demora de tiempo en la carga de los mismos y de esa manera comprobando que la propuesta de mitigación realizada con mod_qos es factible.

Los Gráficos realizados desde 18-3 a la 23-3 se encuentran basados en los datos que se tienen en el Anexo O, al igual que las pruebas estadísticas T-student se encuentran basado de igual manera en los mismos datos. Las pruebas fueron realizadas de igual manera con el tiempo de 1, el puerto 80 y los paquetes que se encuentran en el Anexo K.

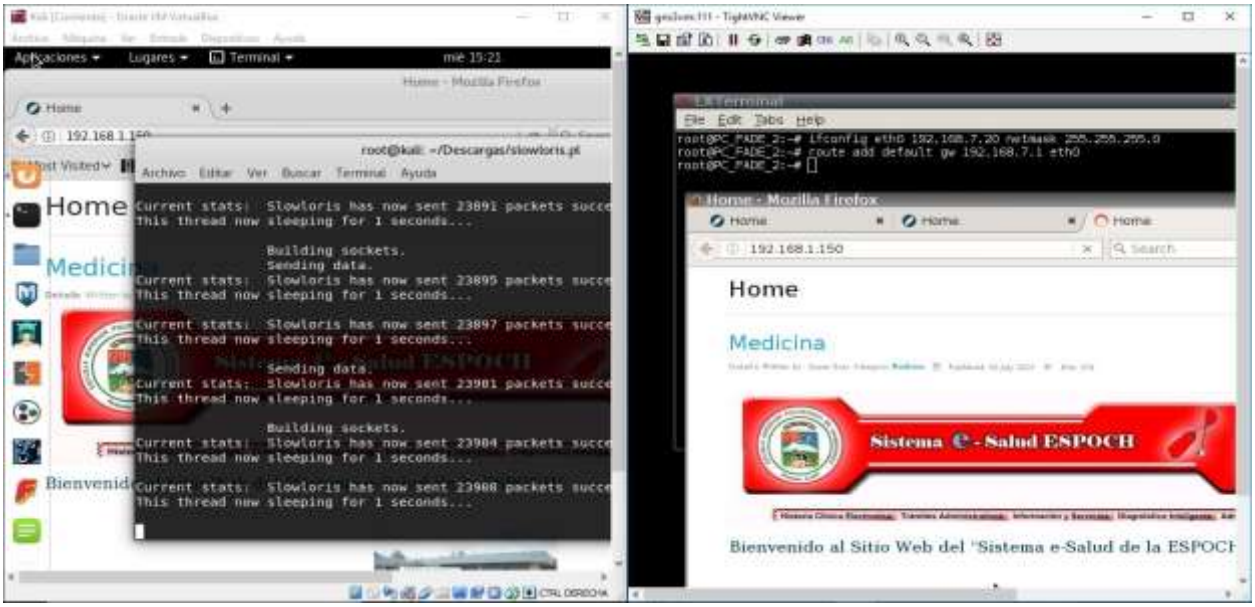



**Figura 22-3:** Ataque DDOS SYN con slowloris instalado mod_qos.

**Realizado por:** Arias, Angel; 2019.

En la figura 39-3 se puede observar la realización del ataque DDOS SYN con slowloris, pero a diferencia de las primeras pruebas en el presente ataque el servidor esta instalado mod_qos y podemos observar que se demora un cierto tiempo, pero nunca existe la denegación del servicio.

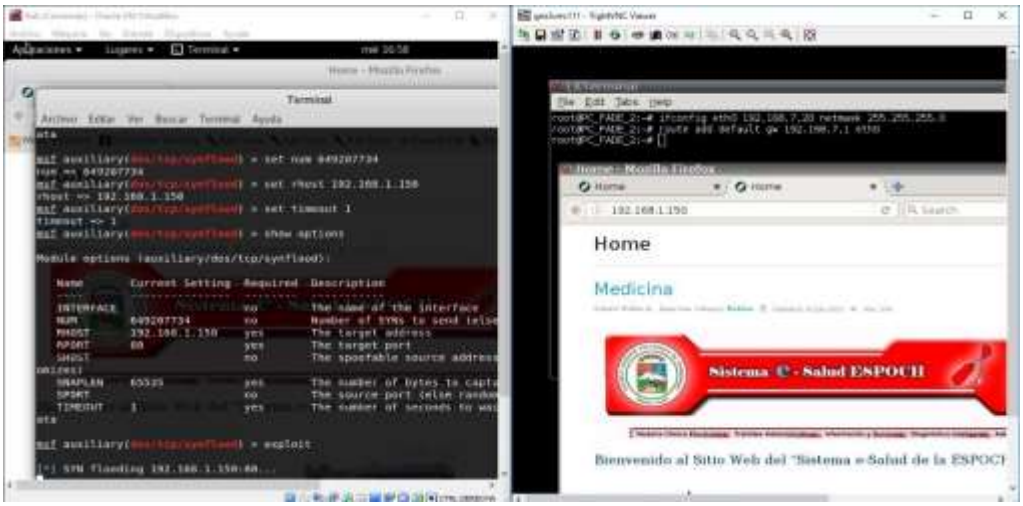



**Figura 23-3:** Ataque DDOS SYN con Metasploit instalado mod_qos.

**Realizado por:** Arias, Angel; 2019.

En la figura 40-3 se observa la realización del ataque DDOS SYN con Metasploit, en donde nunca sucede la denegación de servicio y tiene un tiempo de respuesta más rápido del servicio en comparación del ataque DDOS SYN con slowloris.

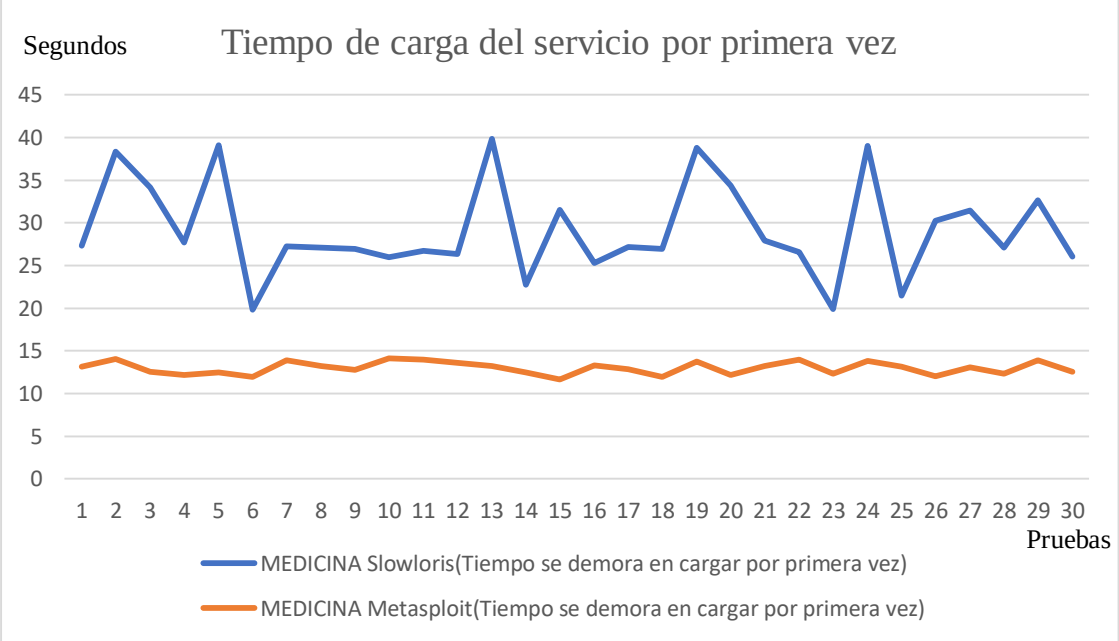



**Gráfico 18-3:** Tiempos de carga del servicio web informativo de medicina durante el ataque DDOS SYN.

**Realizado por:** Arias, Angel; 2019.

**Tabla 7-3:** Prueba T-student con los tiempos de carga por primera vez durante el ataque DDOS SYN en el servicio web informativo de medicina.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 29.2007 | 12.9893 |
| Varianza | 31.9889 | 0.5499 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | 0.2181 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | 16.0231 | |
| P(T<=t) una cola | 0.0000 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 0.0000 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

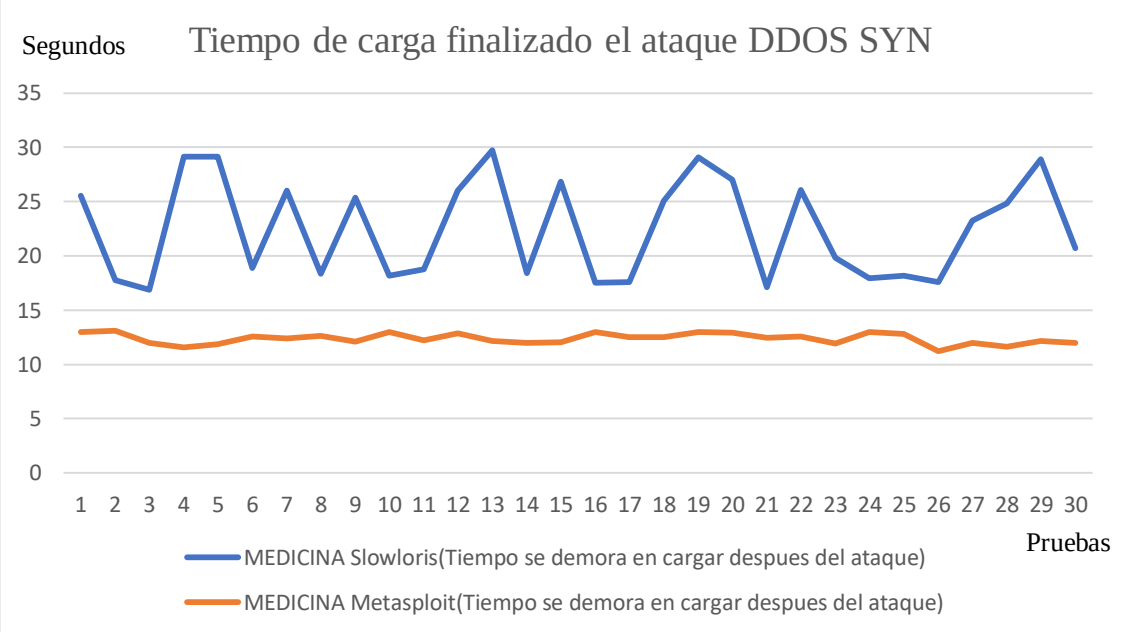



**Gráfico 19-3:** Tiempos de carga finalizado el ataque DDOS SYN en el servicio web informativo de medicina.

**Realizado por:** Arias, Angel; 2019.

**Tabla 8-3:** Tiempos de cargas finalizado el ataque DDOS SYN en el servicio web informativo de medicina.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 22.5263 | 12.3717 |
| Varianza | 21.3182 | 0.2525 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | -0.1455 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | 11.7924 | |
| P(T<=t) una cola | 0.0000 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 0.0000 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

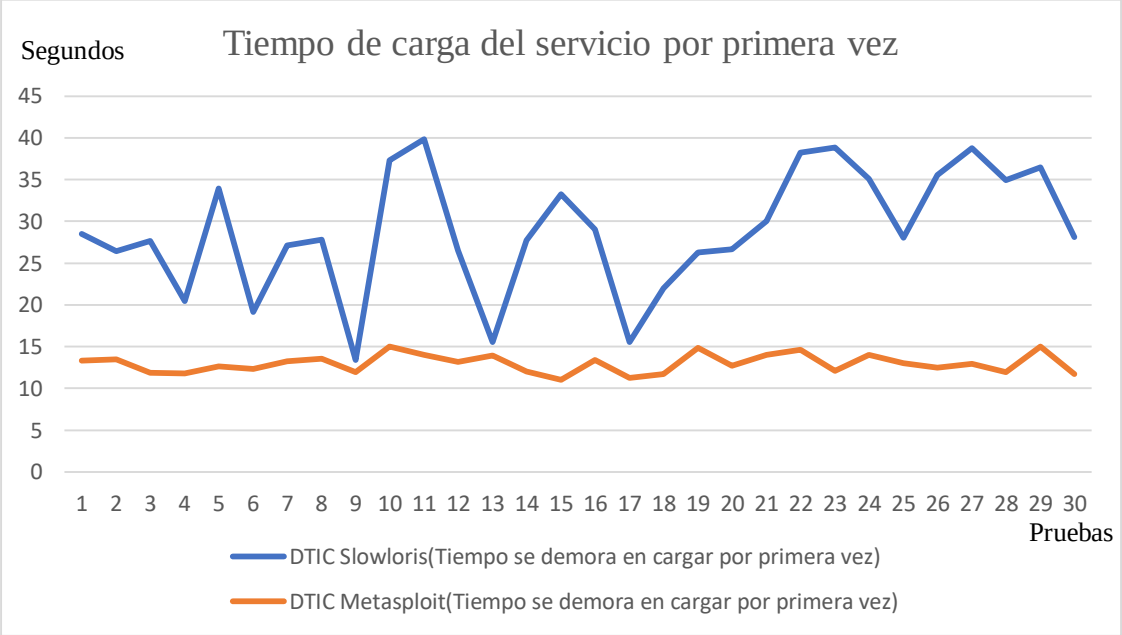



**Gráfico 20-3:** Tiempos de carga del servicio web informativo del DTIC durante el ataque DDOS.

**Realizado por:** Arias, Angel; 2019.

**Tabla 9-3:** Prueba T-student con los tiempos de carga por primera vez durante el ataque DDOS SYN en el servicio web informativo del DTIC.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 28.9413 | 12.9753 |
| Varianza | 53.1274 | 1.2747 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | 0.3560 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | 12.5515 | |
| P(T<=t) una cola | 0.0000 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 0.0000 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

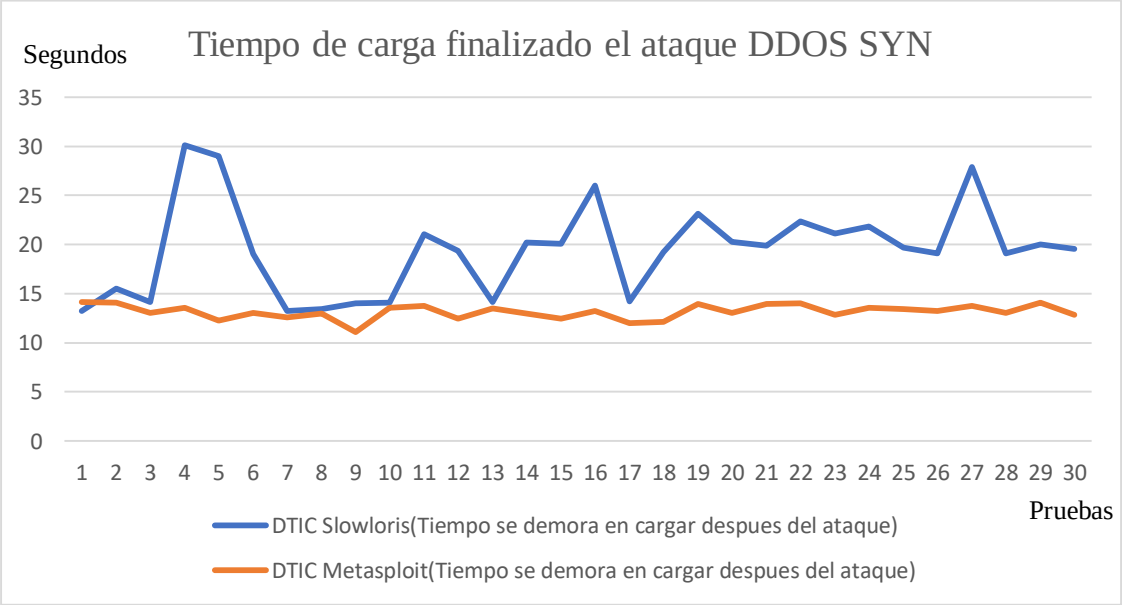



**Gráfico 21-3** Tiempos de carga finalizado el ataque DDOS SYN en el servicio web informativo del DTIC.

**Realizado por:** Arias, Angel; 2019.

**Tabla 10-3:** Tiempos de cargas finalizado el ataque DDOS SYN en el servicio web informativo del DTIC.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 19.4587 | 13.1510 |
| Varianza | 21.5944 | 0.5305 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | 0.1749 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | 7.5497 | |
| P(T<=t) una cola | 0.0000 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 0.0000 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel, 2019.

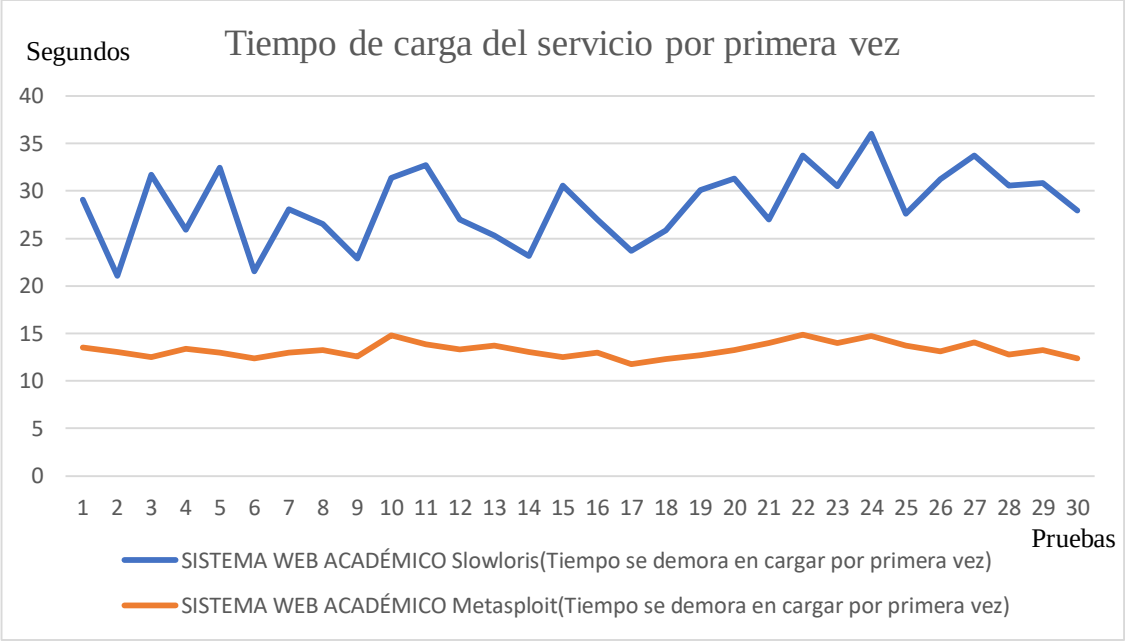



**Gráfico 22-3:** Tiempos de carga del servicio web informativo del sistema web académico durante el ataque DDOS SYN.

**Realizado por:** Arias, Angel; 2019.

**Tabla 11-3:** Prueba T-student con los tiempos de carga por primera vez durante el ataque DDOS SYN en el servicio web informativo del sistema web académico.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 28.5520 | 13.2587 |
| Varianza | 14.5954 | 0.5722 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | 0.5354 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | 24.1077 | |
| P(T<=t) una cola | 0.0000 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 0.0000 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

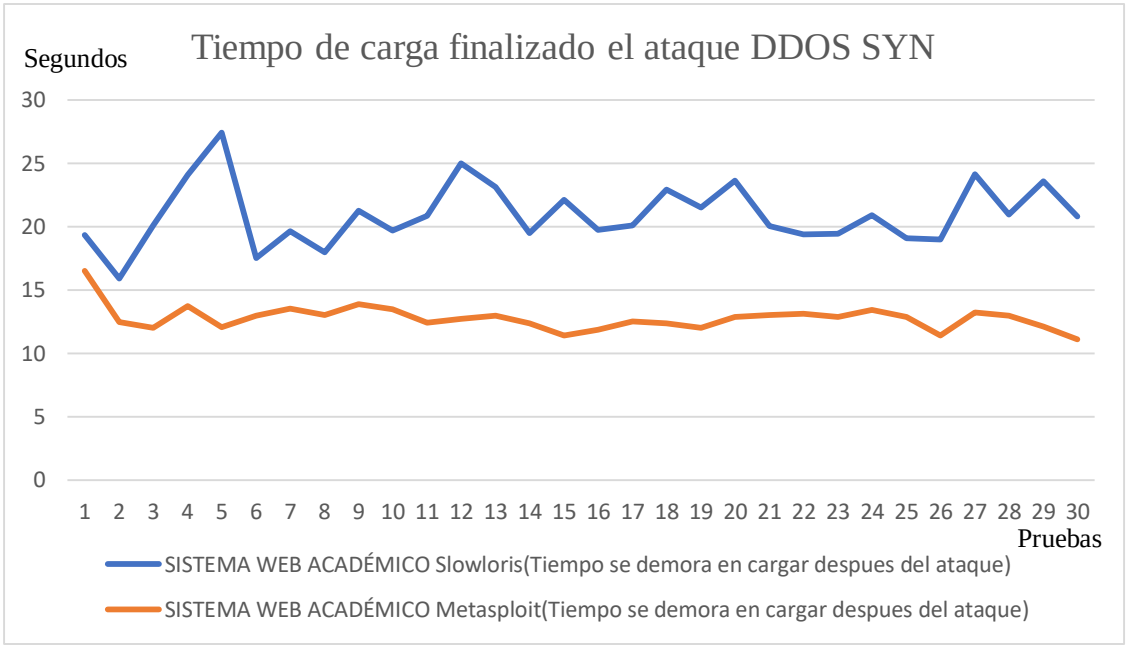



**Gráfico 23-3:** Tiempos de carga finalizado el ataque DDOS SYN en el servicio web informativo del sistema web académico.

**Realizado por:** Arias, Angel; 2019.

**Tabla 12-3:** Tiempos de cargas finalizado el ataque DDOS SYN en el servicio web informativo del sistema web académico.

| Prueba t para medias de dos muestras emparejadas | | |
|---|---|---|
| | | |
| | *Variable 1* | *Variable 2* |
| Media | 20.9630 | 12.7770 |
| Varianza | 5.9728 | 0.9839 |
| Observaciones | 30.0000 | 30.0000 |
| Coeficiente de correlación de Pearson | -0.1015 | |
| Diferencia hipotética de las medias | 0.0000 | |
| Grados de libertad | 29.0000 | |
| Estadístico t | 16.4283 | |
| P(T<=t) una cola | 0.0000 | |
| Valor crítico de t (una cola) | 1.6991 | |
| P(T<=t) dos colas | 0.0000 | |
| Valor crítico de t (dos colas) | 2.0452 | |

**Realizado por:** Arias, Angel; 2019.

Como se puede observar en los Gráficos 18-3, 20-3 y 22-3 se tiene los gráficos del tiempo que se demora en cargar el servicio web informativo de medicina, DTIC y sistema web académico respextivamente, para las 30 pruebas realizadas, en las que se puede observar que el ataque DDOS SYN con slowloris se demora má tiempo en cargar por primera vez a diferencia que el ataque con Metasploit que tiene un tiempo de recarga más rápido en lo que se puede decir que, aun con la solución del mod_qos el ataque con slowloris es más efectivo aunque nunca se produce la denegacion del servicio sino solo se llega a tener un retardo.

Analizando los Gráficos 19-3, 21-3 y 23-3 se tienen los gráficos de los tiempos de respuestas en cargar el servicio web informativo de medicina, DTIC y sistema web académico respectivamente, cuando se finalizó cada uno de los ataques y se puede observar que en cargar el servicio lo hace de manera más rápida el ataque DDOS SYN con Metasploit, en lo que se puede concluir que el ataque más efectivo entre los dos realizados es el ataque DDOS SYN con slowloris, ya que aunque nunca se realizo la denegación del servicio hizo que la carga del mismo sea mas demorado tanto durante y después de la realización del ataque.

En las tablas 7-3, 9-3 y 11-3 se observan las pruebas estadísticas T-student para los servicios web informativos de medicina, DTIC y sistema web académico respectivamente, las cuales se realizaron con los datos que se encuentran en el Anexo O, en donde los datos a analizar son: en primer lugar P(T<=t) dos colas, en donde es igual a 0 lo que quiere decir que se acepta la hipótesis nula y el valor

estáditico t que es positivo, lo que quiere decir que los tiempos de respuesta de la primera carga tanto para el primer ataque como para el segundo son muy parecidos, pero con una pequeña diferencia que el ataque DDOS SYN con slowloris toma un poco más de tiempo que en el servicio web informativo por lo tanto se puede decir que el primer ataque es más efectivo en relación al segundo.

En las tablas 8-3, 10-3 y 12-3 se observan las pruebas estadísticas T-student para los servicios web informativos de medicina, DTIC y sistema web académico respectivamente, en este caso se tiene en cuenta los tiempos de carga del servicio ya habiendo finalizado el ataque DDOS SYN, los análisis se realizaron con los datos que se encuentran en el Anexo O, en donde los datos a analizar son: en primer lugar P(T<=t) dos colas, en donde es igual a 0 lo que quiere decir que se acepta la hipótesis nula y el valor estádistico t que es positivo, lo que representa que los tiempo de carga de cada uno de los servicios web informativos son muy parecidos, pero de igual manera en cargar el servicio toma un poco más de segundos el primer ataque en relación al segundo al que se puede concluir que es mejor el ataque DDOS SYN con slowloris aunque nunca se produjo en ninguno de los dos casos la denegación del servicio gracias a la instalación del mod_qos.

### 3.6. Comparativa del antes con el después

En los Gráficos 24-3, 25-3, 28-3, 29-3, 32-3 y 33-3 se puede observar la comparación de los ataques de denegación de servicio tanto con slowloris como con metasploit, pudiendo observar que, si existe una mejora, en el cual, se trato de mitigar o por lo menos controlar los ataques de denegación de servicio que se realicen en los tres diferentes serivicos web informativos analizados.

La comparación de los tiempos de recarga una vez finalizado los dos tipos de ataques de denegación de servicio diferentes, se pueden observar en los Gráficos 26-3, 27-3, 30-3, 31-3, 34-3 y 35-3, concluyendo que si existe una mejora tanto como cuando se encuentra ejecutándose los dos tipos de ataques, asi como también, cuando se finalizan los mismos el tiempo de carga es menor y con ello se pudo comprobar que la posible solución que se plantea es factible.

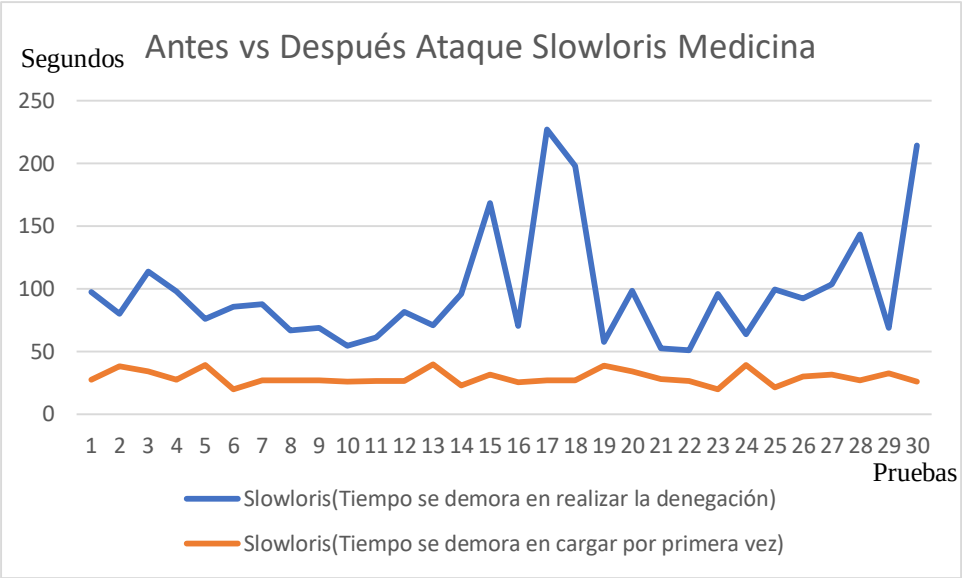



**Gráfico 24-3:** Comparativa del antes con el después del ataque con slowloris en el servicio web informativo de medicina.

**Realizado por:** Arias, Angel; 2019.

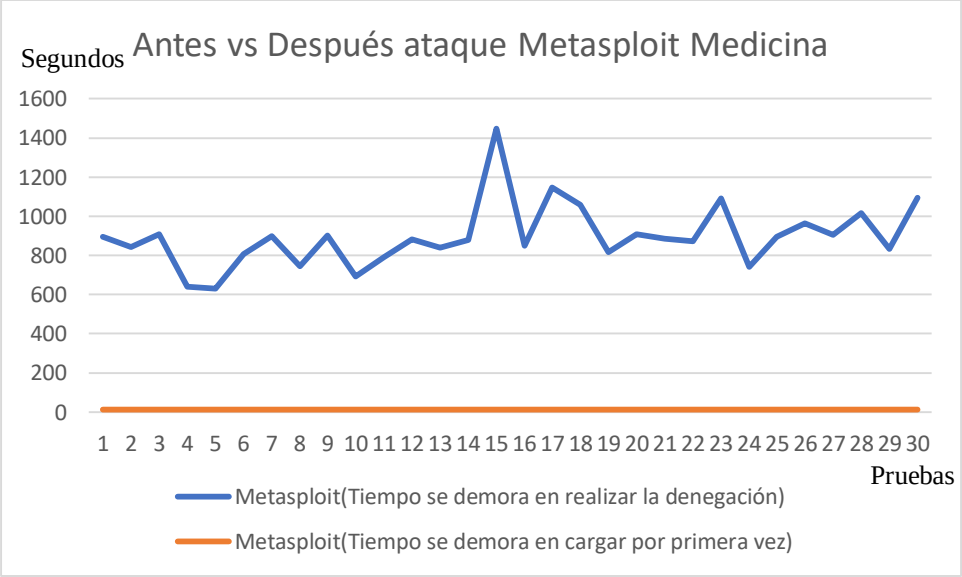



**Gráfico 25-3:** Comparativa del antes con el después del ataque con Metasploit en el servicio web informativo de medicina.

**Realizado por:** Arias, Ángel; 2019.

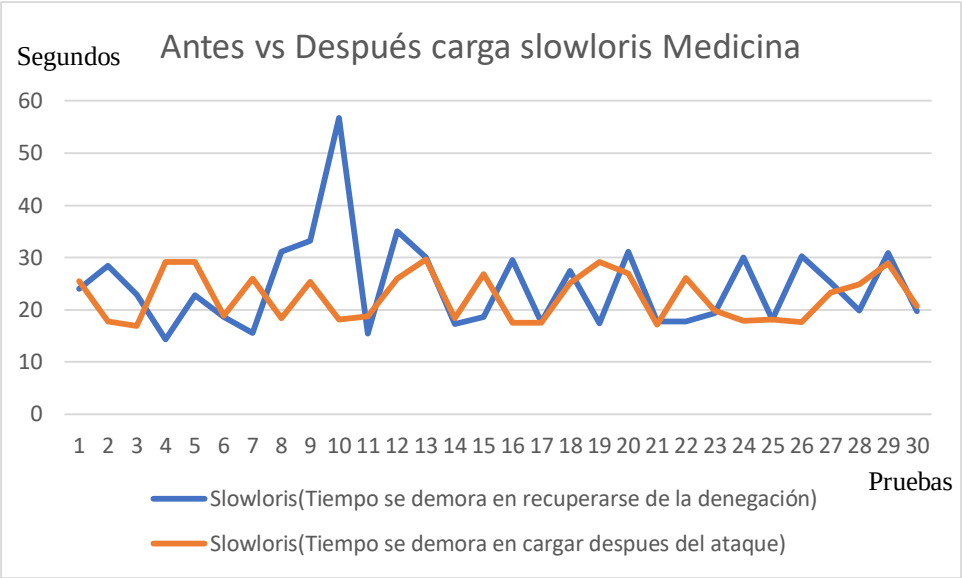



**Gráfico 26-3:** Comparativa en los tiempos de recarga finalizado el ataque con slowloris en el servicio web informativo de medicina.

**Realizado por:** Arias, Ángel; 2019.

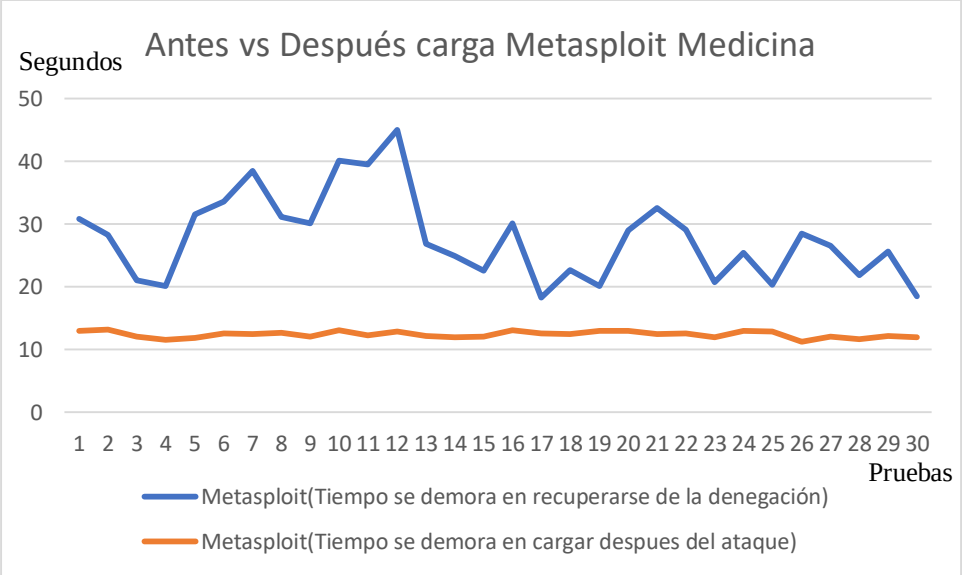



**Gráfico 27-3:** Comparativa en los tiempos de recarga finalizado el ataque con metasploit en el servicio web informativo de medicina.

**Realizado por:** Arias, Ángel; 2019.

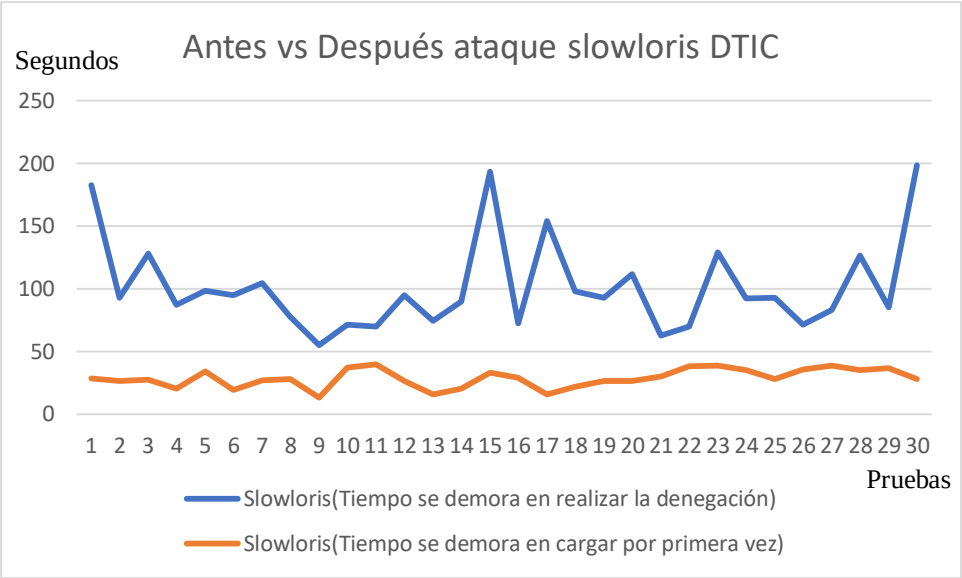



**Gráfico 28-3:** Comparativa del antes con el después del ataque con slowloris en el servicio web informativo del DTIC.

**Realizado por:** Arias, Ángel; 2019.

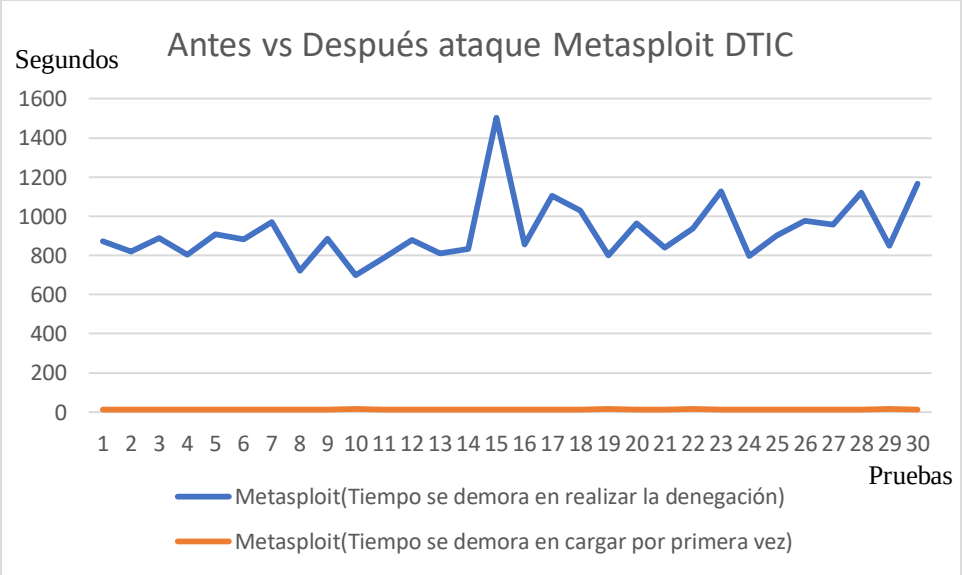



**Gráfico 29-3:** Comparativa del antes con el después del ataque con Metasploit en el servicio web informativo de DTIC.

**Realizado por:** Arias, Ángel; 2019.

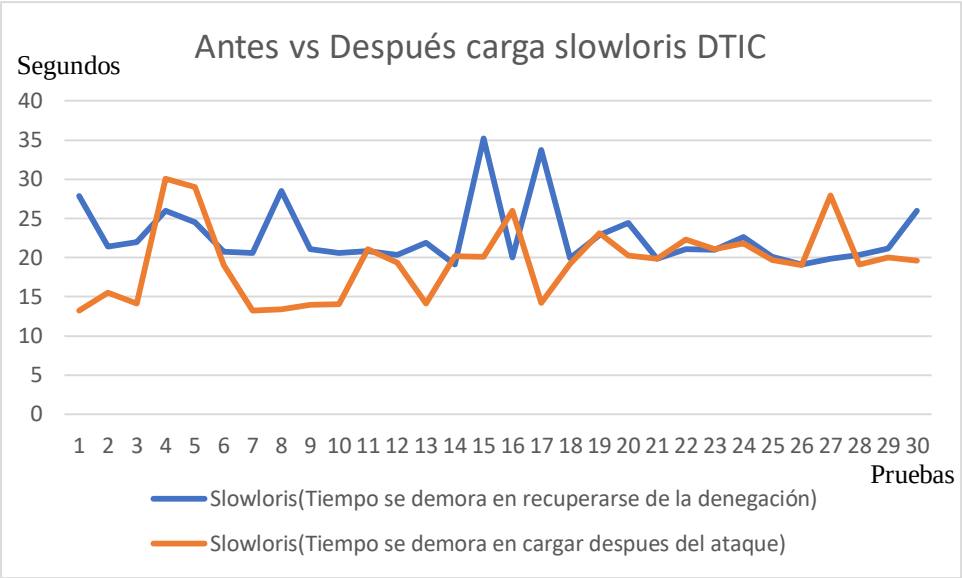



**Gráfico 30-3:** Comparativa en los tiempos de recarga finalizado el ataque con slowloris en el servicio web informativo del DTIC.

**Realizado por:** Arias, Ángel; 2019.

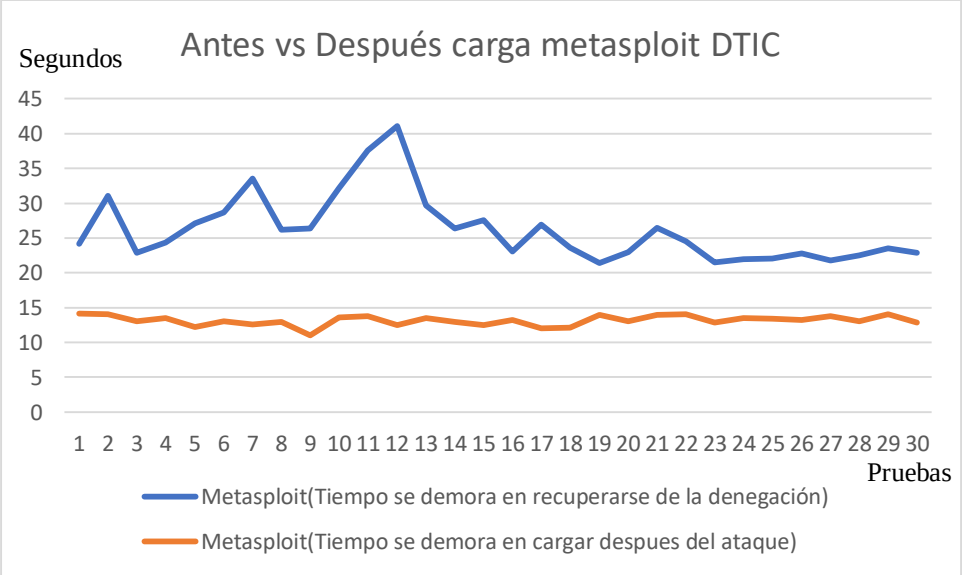



**Gráfico 31-3:** Comparativa en los tiempos de recarga finalizado el ataque con metasploit en el servicio web informativo del DTIC.

**Realizado por:** Arias, Ángel; 2019.

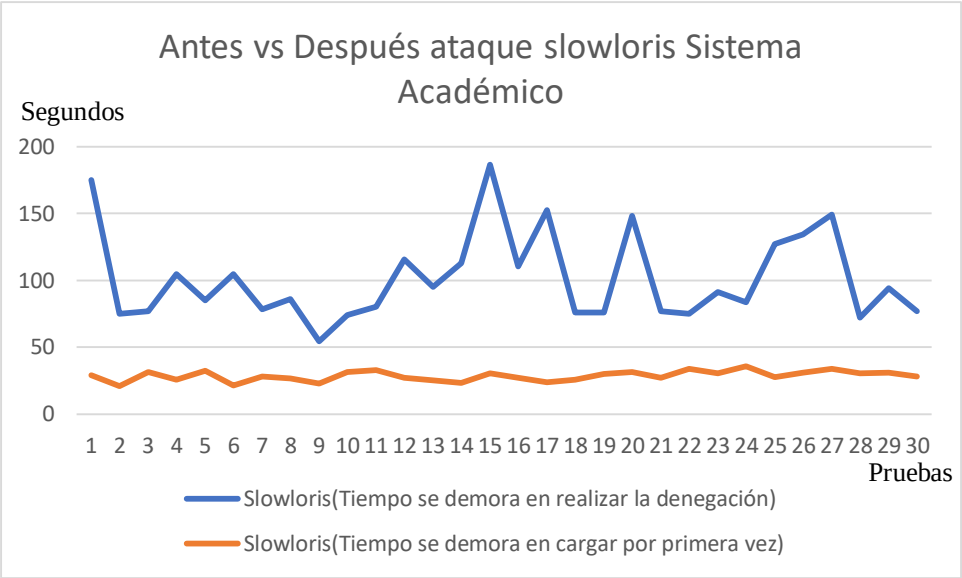



**Gráfico 32-3:** Comparativa del antes con el después del ataque con slowloris en el servicio web informativo del sistema académico.

**Realizado por:** Arias, Ángel; 2019.

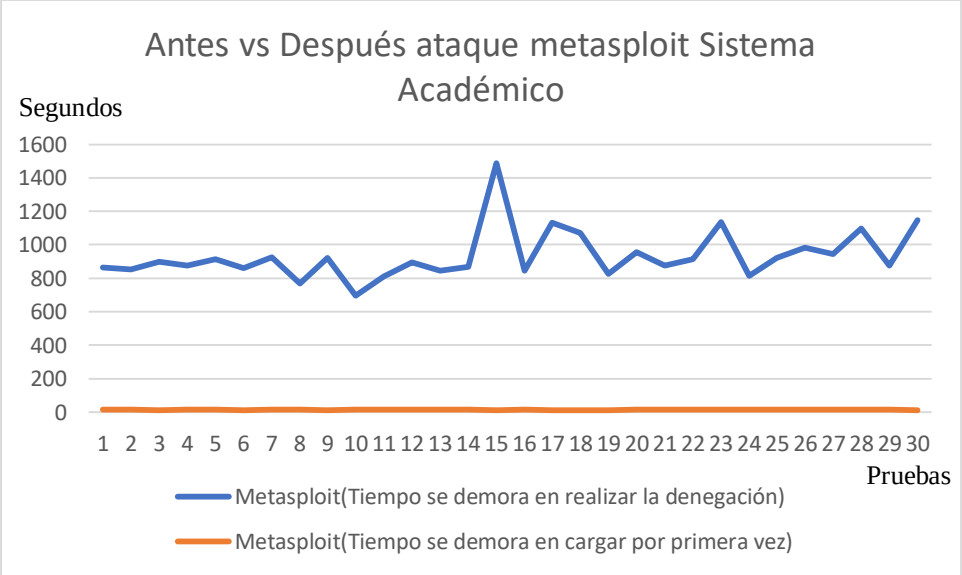



**Gráfico 33-3:** Comparativa del antes con el después del ataque con Metasploit en el servicio web informativo del sistema académico.

**Realizado por:** Arias, Ángel; 2019.

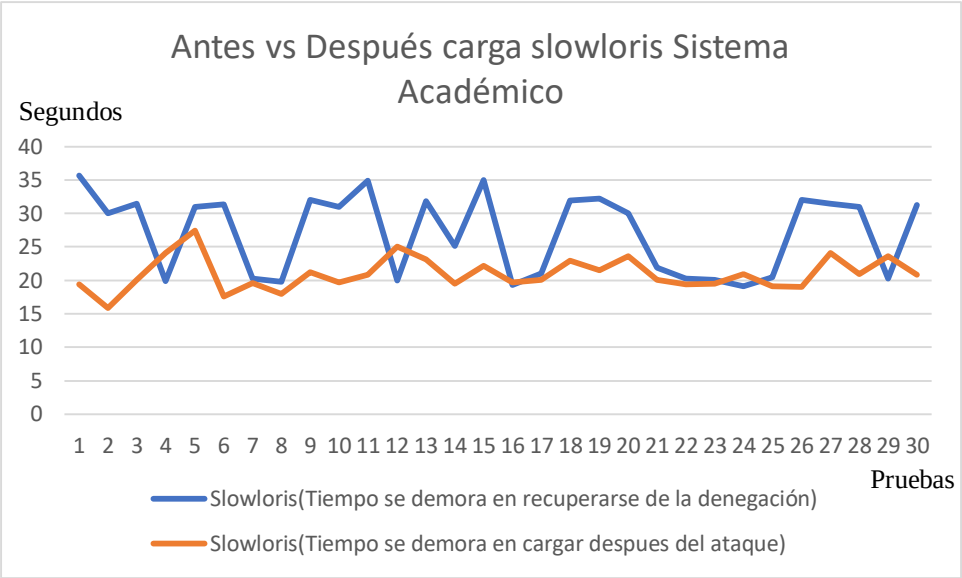



**Gráfico 34-3:** Comparativa en los tiempos de recarga finalizado el ataque con slowloris en el servicio web informativo del sistema académico.

**Realizado por:** Arias, Ángel; 2019.

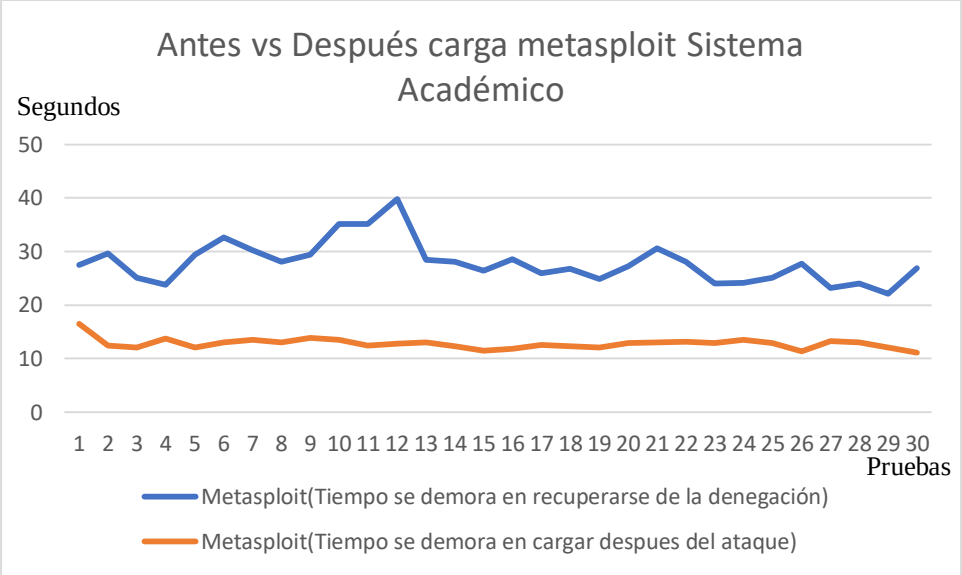



**Gráfico 35-3:** Comparativa en los tiempos de recarga finalizado el ataque con metasploit en el servicio web informativo del sistema académico.

**Realizado por:** Arias, Ángel; 2019.

# CAPITULO IV

## 4. METODOLOGÍA HÍBRIDA

En el presente capitulo se detalla y muestra la metodologiía hibrida que se realizo teniendo en cuenta las diferentes metodologías que se planteo analizar las cuales son: NIST 800 – 144, ISSAFF, OSSTMM y OWASP.

### 4.1. Introducción

La presente metodología se encuentra basado en varias metodologías existentes para el análisis de servidores virtuales, la cual se encuentra diseñada para evaluar la red, los sistemas y aplicaciones de control. Se ha tomado como punto de partida las metodologías NIST 800 – 144, Information Systems Security Assessment Framework (ISSAF), Open Web Application Security Project (OWASP) y The Open Source Security Testing Methodology Manual (OSSTM), dado que no existe una metodología en específico para el análisis de servidores virtuales. de acuerdo a OISSG (2006). Las etapas que se utilizaran para el presente análisis cual se encuentra dividido en tres fases, las cuales son:

- Fase 1: Planificación
- Fase 2: Desarrollo
- Fase 3: Resultados

#### *4.1.1. Fase 1: Planificación*

En la presente fase lo que se realiza es un acuerdo de confidencialidad entre el asesor y la empresa para que no exista divulgación de la información, se establecen los límites para el análisis de vulnerabilidades y se aceptan los recursos necesarios tanto del usuario como de la empresa para que se encuentren en un mutuo acuerdo. (OISSG, 2006, p. 13).

### *4.1.2. Fase 2: Desarrollo*

De acuerdo a OISSG (2006). Se empieza a realizar el análisis de vulnerabilidades de los servidores virtuales tomando como partida siete pasos los cuales son:

- Recolección de la información.
- Definición de la red a analizar.
- Identificación de vulnerabilidades que poseen los servidores virtuales.
- Explotación de las vulnerabilidades
- Comprobación de explotación de vulnerabilidades
- Implementación de mejoras para mitigar vulnerabilidades.
- Explotación y verificación de las vulnerabilidades corregidas.

En el siguiente diagrama se puede observar las fases y pasos que se realizan para asegurar las vulnerabilidades de los servidores virtuales, se puede usar de la manera cíclica para tener la seguridad de los servidores virtuales de la manera más óptima. (OISSG, 2006, p. 13).

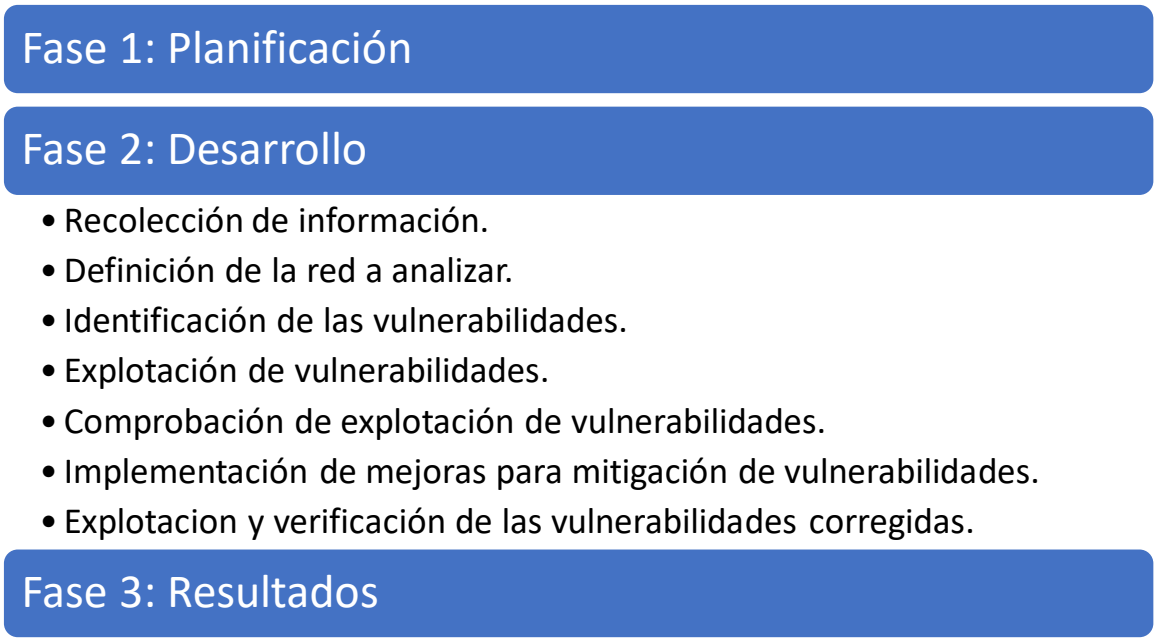



**Gráfico 1-4:** Etapas para el análisis de vulnerabilidades de servidores virtuales.

**Realizado por:** Arias, Ángel; 2019.

#### *4.1.2.1. Recolección de información*

La recolección es muy fundamental, para poder conocer los tipos de servidores virtuales que posee la empresa en la que se desea realizar el estudio, conocer en qué sistema/s operativo/s se encuentran corriendo los diferentes servidores virtuales, para poder recolectar información se puede utilizar dos métodos los cuales son: método técnico (DNS/WHOIS) y el no técnico (buscar ingenieros, grupos, foros, etc.). (OISSG, 2006, p. 16).

Este es el paso inicial en cualquier auditoria de seguridad. La información se puede recolectar desde lugares públicos o internet, es muy importante ya que el asesor tiene el tiempo y los recursos limitados. Y a la par de poder identificar los puntos más importantes que se puede tener en las vulnerabilidades. (OISSG, 2006, p. 16).

#### *4.1.2.2. Definición de la red a analizar*

Después de haber recolectado toda la información posible, aquí se plantea una posible red muy similar dado que no puede ser parecida por motivos de confidencialidad de la empresa a la cual se le esta realizando la auditoria de las vulnerabilidades de los servidores virtuales. (OISSG, 2006, p. 16).

En este punto se pueden utilizar varios softwares asi como también aplicaciones, o técnicas de recolección de información sobre los hosts y redes que se encuentren involucradas en el análisis. (OISSG, 2006, p. 16).

De acuerdo a OISSG (2006). Se puede tener varios puntos en cuenta como son:

- Encontrar anfitriones en vivo.
- Identificación de los puertos a escanear.
- Perímetro de la red, que routers, firewalls, entre otras características posee la red a analizar.
- Identificación de los servicios que se tienen en los servidores virtuales.
- Sistemas operativos que utilizan los servidores virtuales. (OISSG, 2006, p. 16-17).

En el caso de que no se tenga acceso a la infraestructura, se realizara una simulación con la red propuesta en los diferentes softwares de simulación como pueden ser: GNS3, Packet tracer, entre otros. Y en el ambiente simulado realizar todas las pruebas necesarias para el análisis de vulnerabilidades de los servidores virtuales que posee la empresa. (OISSG, 2006, p. 17).

#### *4.1.2.3. Identificación de las vulnerabilidades que poseen los servidores virtuales*

En esta parte se identifican las vulnerabilidades que poseen los servidores virtuales, estas vulnerabilidades varian dependiendo en que se encuentran levantados como puede ser: php, mysql, etc. (OISSG, 2006, p. 17) De acuerdo a OISSG (2006). En el cual para poder realizar dicha identificación se realizarán las siguientes actividades:

- Identificación de los servicios vulnerables
- Escaneo de puertos para comprobación de las vulnerabilidades de los servidores virtuales.
- Verificación si las vulnerabilidades dan un resultado afirmativo o negativo.
- Enumeración de las vulnerabilidades encontradas.
- Estimación del posible impacto de las vulnerabilidades.
- Identificación de los ataques y escenarios para la explotación. (OISSG, 2006, p. 17).

#### *4.1.2.4. Explotación de vulnerabilidades*

El asesor trata de ganar acceso no autorizado a los servicios que ofrecen los servidores virtuales, se pueden seguir los siguientes pasos: (OISSG, 2006, p. 17).

- Identificación del código en el que se encuentran los servidores virtuales.

De acuerdo a OISSG (2006). Aquí se refiere en que sistema operativo se encuentran dichos servidores, y según el sistema operativo que tipo de kernel posee para de esa manera obtener privilegios que no son permitidos.

- Identificación de las aplicaciónes instaladas en los servidores virtuales.
- Desarrollo de scripts.
- Prueba del código de los sistemas operativos de los servidores virtuales
- Explotación de las vulnerabilidades de las aplicaciones. (OISSG, 2006, p. 17-18).

#### *4.1.2.5. Obtención de privilegios y escalabilidad.*

De acuerdo a OISSG (2006), se trata de obtener los privilegios más altos para de esa manera poder tener un mayor conocimiento de los servidores virtuales, los parámetros que se identifican son:

- Descubrimiento de usuario y contraseña. Se pueden utilizar varios ataques como son fuerza bruta, diccionarios, entre otros.
- Descubrimiento de la clave por defecto del sistema.
- Explotación de la configuración por defecto del proveedor.
- Descubrimiento de los servicios que se tienen en los servidores virtuales, permitiendo escribir, crear y eliminar los servicios. (OISSG, 2006, p. 18-19).

#### *4.1.2.6. Comprobación de explotación de vulnerabilidades*

En el presente paso se realiza la comprobación del análisis de vulnerabilidades, si fue exitoso o no. En el cual se puede tomar en cuenta los siguientes puntos:

- Obtención de claves
- Lectura del tráfico y los servicios web que acceden los usuarios
- Identificación de la red y rutas.
- Obtención de acceso a los servicios web como root.
- Modificación de los servicios web en los servidores virtuales. (OISSG, 2006, p. 19-20).

Los puntos anteriormente mencionados ayudan para poder verificar de manera positiva o negativa si la auditoria del análisis de vulnerabilidades.

#### *4.1.2.7. Implementación de mejoras para mitigación de vulnerabilidades*

Aquí el asesor se encarga de realizar las mejoras que vea pertinentes según las vulnerabilidades que se hayan encontrado en la auditoria. Se pueden utilizar varias aplicaciones o softwares como el asesor vea conveniente, como pueden ser: Honeypot, firewalls, el bloqueo de direcciones IP para evitar ataques de denegación de servicio, cerrar los puertos, entre otras aplicaciones que se vean oportunas. (OISSG, 2006, p. 20).

Para evitar varias fallas se tiene algunos parámetros que se pueden cumplir para que el asesor confirme la seguridad de los servidores virtuales como son:

- Mantener actualizados los antivirus, en caso de no tener uno instalar un antivirus.
- Tener actualizado el software de los sistemas operativos.

- Si se requiere ingresar a un servicio que solicite clave, en la contraseña que no se permita utilizar comillas simples y/o comillas dobles.

Cuando se ingresa una clave se trata de evitar tanto las comillas simples como las comillas dobles porque si permitimos que el usuario introduzca libremente cualquier texto en el área de la contraseña sin ninguna restricción, puede llegar a aprovecharse y tener acceso a la base de datos que se tenga. (OISSG, 2006, p. 20).

#### *4.1.2.8. Explotación y verificación de las vulnerabilidades corregidas*

En el último apartado de la presente metodología lo que se realizan son los pasos que se realizaron para la auditoria de análisis de vulnerabilidades de los servidores virtuales, el presente análisis se ejecuta después de realizar todas las mejoras que el asesor vea pertinente para poder asegurar la información que se tienen en los servidores virtuales. (OISSG, 2006, p. 21).

### ***4.1.3. Fase 3: Resultados***

Para que informar a la empresa de los resultados obtenidos se tienen los siguientes puntos como referencia:

#### *4.1.3.1. Reporte verbal*

En el presente paso, si en el momento que se esté realizado la auditoria de los servidores virtuales, se debe avisar a la empresa de la manera más rápida posible, en el que se pondrá de acuerdo el asesor con la empresa para poder realizar los cambios más óptimos de manera inmediata para asegurar los servicios que se tengan en los servidores virtuales. (OISSG, 2006, p. 23).

#### *4.1.3.2. Reporte final*

Al finalizar todos los pasos de la auditoria de los servidores virtuales, se procede a realizar un escrito para informar a la empresa todas las vulnerabilidades que se encontraron, así como también las

medidas y aplicaciones que se tomaron para poder realizar la mitigación de las vulnerabilidades encontradas (OISSG, 2006, p. 23). De acuerdo a OISSG (2006) se deben poner los siguientes puntos:

- Resumen de la auditoria.
- Puertos analizados.
- Pruebas realizadas.
- Tiempo de las pruebas realizadas.
- Puertos escaneados.
- Lista de vulnerabilidades encontradas.
- Lista de acciones tomadas para mitigar las vulnerabilidades encontradas. (OISSG, 2006, p. 23-24).

Las presentes fases y pasos que se han seleccionado para el análisis de vulnerabilidades de servidores virtuales se ha tomado de la metodología Information Systems Security Assessment Framework (ISSAF), dado que se tiene tanto seguridad para el asesor como para la empresa y sus activos, realizando acuerdos y delimitando hasta donde se puede llegar según vea pertinente la empresa. Se realiza de una forma adecuada el desarrollo de la asesoría, informando en caso inmediato de ser necesario y entregando un informe final a la empresa en todo lo que se realizó. (OISSG, 2006, p. 24)

### 4.2. Que se debe conocer

El presente manual trata sobre el análisis de las vulnerabilidades de los servidores virtuales, en el cual se puede mencionar OpSec lo cual es una combinación de la separación y controles, en el cual se trata de tener mayor número de interacciones ya que directa o indirectamente que se tengan con el activo, si se separa al atacante del activo se puede decir que se tiene una seguridad total. En caso de que no exista dicha separación total, lo que se tiene es la seguridad de los controles que se tengan realizadas en el cual se disminuye el grado de impacto de la amenaza. (ISECOM, 2017, p. 20)

Para poder tener una verdadera seguridad, se plantean varios puntos de control para proteger los activos. Aunque si se tiene mayor número de controles puede que exista también mayores interacciones entre el atacante con el activo, lo que quiere decir que no se tiene más segura la información mientras se tengan mayor número de controles. Para ello se debe conocer algunas terminologías como son: (ISECOM, 2017, p. 20).

### *4.2.1. Seguridad*

La seguridad se le conoce como una función de una separación. En el cual se separa el activo y cualquier amenaza de si existe o no. (ISECOM, 2017, P.23) De acuerdo a ISECOM (2017), se tienen 3 formas lógicas y proactivas para poder realizar dicha separación las cuales son:

- Mover el activo para crear una barrera entre el mismo y sus amenazas.
- Cambiar la amenaza a un estado inofensivo
- Destruir la amenaza

Cuando se realiza la auditoria de los servidores virtuales, se puede conocer todo, un poco o nada de las interacciones que se tengan entre el activo y sus amenazas. Para la seguridad se toman en cuenta tres elementos importantes: visibilidad, acceso y confianza, lo cual permite al asesor agregar los controles adecuados durante la auditoria. (ISECOM, 2017, P.23)

**Tabla 1-4:** Definición de elementos de la seguridad.

| **Término** | **Concepto** |
|---|---|
| Visibilidad | La visibilidad es un medio para calcular la oportunidad, conociéndose la oportunidad como un elemento que fomenta el robo, junto con beneficio y riesgo disminuido. Es el activo que conoce el atacante que puede se encuentra dentro de su alcance, dado que lo que no conoce no puede ser atacado. |
| Acceso | El acceso es el número de lugares en donde puede existir la interacción del atacante con el activo. |
| Confianza | Se mide la confianza como parte de OpSec, ya que cada interacción que existe el asesor las acepta libremente los objetivos. En donde se recomienda el uso de métricas para la confianza, permitiendo medir el nivel de confianza que se tenga. |

**Fuente:** ISECOM, 2017, p. 23.

**Realizado por:** Arias, Angel; 2019.

### *4.2.2. Controles*

Los controles son utilizados cuando el atacante se encuentra en la red, para poder asegurar los activos que se manejen en los servidores virtuales, lo cual permite influir en el impacto que se tendrá respecto a la amenaza. En el cual se pueden destacar dos tipos de controles los cuales son: (ISECOM, 2017, P.24)

#### *4.2.2.1. Controles interactivos*

Los presentes controles constituyen la mitad de todos los procesos de la operación. Los cuales influyen directamente en la visibilidad, el acceso o las interacciones de confianza. (ISECOM, 2017, P.25) De acuerdo a ISECOM (2017), las categorías que se tienen en el presente plano de control son:

- **Autenticación:** es un control el cual se encuentra basado en la identificación y la autorización.
- **Indemnización:** es un control que se tiene entre el asesor y la empresa. Puede tener la forma de una advertencia de si no se siguen las reglas de confidencialidad que se estipulo con la empresa a la que se le está realizando la auditoria.
- **Resiliencia:** es un control destinada a las interacciones que se tenga, para poder mantener los activos protegidos en caso de que exista alguna falla.
- **Subyugación:** es un control el cual garantiza a la empresa que las interacciones que se tengan están bajos los parámetros delimitados, en la cual la empresa propietaria de los activos define hasta que tipo de interacciones se puede tener y cuál es la consecuencia en caso de pérdida.
- **Continuidad:** es un control destinado a que se mantenga las interacciones con los activos en caso de que exista alguna falla.

#### *4.2.2.2. Procesos de control*

La otra mitad de los controles, son los procesos de control los cuales son utilizados para crear procesos defensivos. En este tipo de controles no se tiene en cuenta las interacciones que se tengan, sino que protegen los activos cuando la amenaza ya está presente. (ISECOM, 2017, P.25) De acuerdo a ISECOM (2017), los parámetros que se tienen para estos controles son:

- **No repudio:** es un control que se tiene para que ninguna de las partes pueda negar las interacciones que se tengan.
- **Confidencialidad:** es un control que permite que cualquier activo que se tenga la empresa, el asesor no lo puede hacer público a personas o empresas externas.
- **Privacidad:** es un control para poder asegurar de cómo se accede, se muestra o se intercambia la información entre asesor y la empresa y no se pueda conocer dicha información fuera de estas partes.
- **Integridad:** es un control que se utiliza para conocer el asesor y la empresa cuando la información ha tenido un cambio.

- **Alarma:** es un control que informa las interacciones que han ocurrido.

El uso de controles debe asegurar de que no exista nuevos objetivos de ataques, por lo cual en circunstancias es mejor no tener tantos controles ya que puede realizarse un mal control y puede generar mayores visibilidades de los activos para que puedan atacar. (ISECOM, 2017, P.25).

### *4.2.3. Objetivos de la información*

Los objetivos de la información más importantes para los servicios que ofrecen los servidores virtuales son: confidencialidad, integridad y la disponibilidad. (ISECOM, 2017, P.27) De acuerdo a ISECOM (2017), los controles que se tienen para poder cumplir cada objetivo se le puede observar en la siguiente tabla:

**Tabla 2-4:** Relación de los objetivos de la información y los controles.

| **Objetivos de la información** | **Controles** |
|---|---|
| Confidencialidad | Confidencialidad<br>Privacidad<br>Autenticación<br>Resiliencia |
| Integridad | Integridad<br>No repudio<br>Subyugación |
| Disponibilidad | Continuidad<br>Indemnización<br>Alarma |

**Fuente:** ISECOM, 2017, p. 27.

**Realizado por:** Arias, Angel; 2019

### *4.2.4. Limitaciones*

A las limitaciones se le denomina como el estado de seguridad con respecto a las fallas y restricciones. Son los agujeros, vulnerabilidades, debilidades y problemas para mantener la separación entre el activo y una amenaza, o para que los controles continúen funcionando correctamente. (ISECOM, 2017, P.28)

Las limitaciones se han clasificado en cinco categorías, las cuales definen el tipo de vulnerabilidad, error, mala configuración o deficiencia cuando estén ejecutándose los servicios que ofrecen los servidores virtuales. dado que no se puede conocer la cantidad de amenazas, es más factible para el asesor realizar un mecanismo basado en cuando fallaran. Lo cual permitirá realizar pruebas de las condiciones cuando ya no se tendrá el nivel de protección necesario. (ISECOM, 2017, P.28)

Las 5 categorías de limitaciones que se explican a continuación, su jerarquía depende de la información y de los servicios que se estén ofreciendo en los servidores virtuales, dando con ello mayor relevancia a cada una según sea la situación. (ISECOM, 2017, P.28) De acuerdo a ISECOM (2017), las categorías son:

- **Vulnerabilidad:** para poder definir las vulnerabilidades se tienen tres conceptos distintos los cuales son: denegación de acceso a los activos a personas o procesos autorizados, permite el ingreso a los activos a personas o procesos no autorizados y permite que personas o procesos no autorizados oculten los activos o a sí mismos.
- **Debilidad:** es la falla en la cual interrumpe, reduce, abusa o anula específicamente los cinco controles interactivos que son: autenticación, indemnización, resiliencia, subyugación y continuidad. (ISECOM, 2017, P.29)
- **Preocupación:** es la falla en la cual interrumpe, reduce, abusa o anula específicamente los cinco procesos de control que son: no repudio, confidencialidad, privacidad, integridad y alarma. (ISECOM, 2017, P.29)
- **Exposición:** es una falla que no se permite, la cual se refiere a la visibilidad de los objetivos o activos de los servicios en los servidores virtuales. Da información sobre la interacción con un objetivo, la cual se puede utilizar en ambas clases de control. La exposición en si no tiene ningún valor, a menos de que exista una forma de poder explotar el activo o los procesos de los servicios que ofrecen los servidores virtuales, por lo cual en esas circunstancias, las vulnerabilidades desempeñan un papel importante en la exposición. (ISECOM, 2017, P.29)
- **Anomalía:** es un elemento que no se ha podido identificar o desconocido que no se ha podido controlar y no se puede contabilizar en operaciones normales. (ISECOM, 2017, P.29)

A continuación, en la siguiente tabla se puede observar la asignación de la seguridad y las limitaciones que encajan con el marco de OpSec:

**Tabla 3-4:** Relaciones entre categorías, OpSec y limitaciones.

| **Categoría** | | **OpSec** | **Limitaciones** |
|---|---|---|---|
| Operaciones | | Vulnerabilidad | Exposición |
| | | Acceso<br>Confianza | Vulnerabilidad |
| Controles | Procesos interactivos | Autenticación<br>Indemnización<br>Resiliencia<br>Subyugación<br>Continuidad | Debilidad |
| | Procesos de control | No repudio<br>Confidencialidad<br>Privacidad<br>Integridad<br>Alarma | Preocupación |
| | | | Anomalías |

**Fuente:** ISECOM, 2017, p. 29.

**Realizado por:** Arias, Angel; 2019.

### 4.3. Auditoria de vulnerabilidades

De acuerdo a ISECOM (2017), para poder iniciar el análisis de vulnerabilidades de los servidores virtuales se toman en cuenta algunos puntos de partida los cuales son:

- Definir que se desea proteger. La información que se desea proteger, así como las limitaciones que se tendrá para realizar el análisis de vulnerabilidades.
- Identificar los mecanismos de protección y controles que se tienen creados para proteger los activos que se ofrecen en los servicios de los servidores virtuales.
- Definir como los servicios de los servidores virtuales interactúan con los usuarios que tienen acceso a los mismos.
- Identificar qué equipo/s y que software será necesario para realizar cada prueba. En caso de no tener acceso de manera física a los servidores virtuales, identificar que software su utilizara para

su simulación. Y determinar que parámetro se tendrán en cuanta entre los que se tiene: humano, físico, inalámbrico, telecomunicaciones y redes de datos.

- Identificar qué información se quiere aprender del análisis de vulnerabilidades de servidores virtuales. y determinar qué tipo de análisis se realizará los cuales se han definido en seis tipos los cuales son: ciego, doble persiana, caja gris, doble caja gris, tándem y reversa.
- Asegurar que las pruebas que se realizaron cumple con los compromisos de confidencialidad que se acordaron con la empresa, para que no exista ningún problema en el futuro. (ISECOM, 2017, P.33)

### *4.3.1. Parámetros*

En la siguiente tabla se puede observar de manera más detallada los parámetros que se deben identificar y cuales se piensan utilizar según sea el caso necesario: (ISECOM, 2017, P.34)

**Tabla 4-4:** Definición de los parámetros que se deben identificar.

| **Parámetros** | **Definición** |
|---|---|
| Humano | Comprende el ámbito humano, aquí se tiene en cuenta la interacción tanto física como psicológica. Este parámetro es muy utilizado cuando se tiene acceso a los equipos de manera real. |
| Físico | Pruebas de seguridad de los equipos que se tienen, para asegurarse que todos los equipos cuentan con las seguridades necesarias. |
| Inalámbrico | Comprende todas las comunicaciones electrónicas que se tengan, en caso de que sea simulado comprende las peticiones que se realizan desde las máquinas virtuales a los servicios de los servidores virtuales simulados. |
| Telecomunicaciones | Comprende la red y como está diseñada, en el caso de que se realice una simulación el escenario debe ser muy similar al real, no real por temas de confidencialidad de la empresa. |
| Redes de datos | Es toda la información que el asesor desea analizar tanto en el ámbito físico como puede ser en el simulado, con la finalidad de mitigar las vulnerabilidades existentes. |

**Fuente:** ISECOM, 2017, p. 35

**Realizado por:** Arias, Angel; 2019.

### *4.3.2. Tipo de pruebas*

En la siguiente figura se puede observar un esquema para comprender de mejor manera el tipo de análisis al que se tenga acceso o el que desee realizar el asesor con los servidores virtuales: (ISECOM, 2017, P.36).

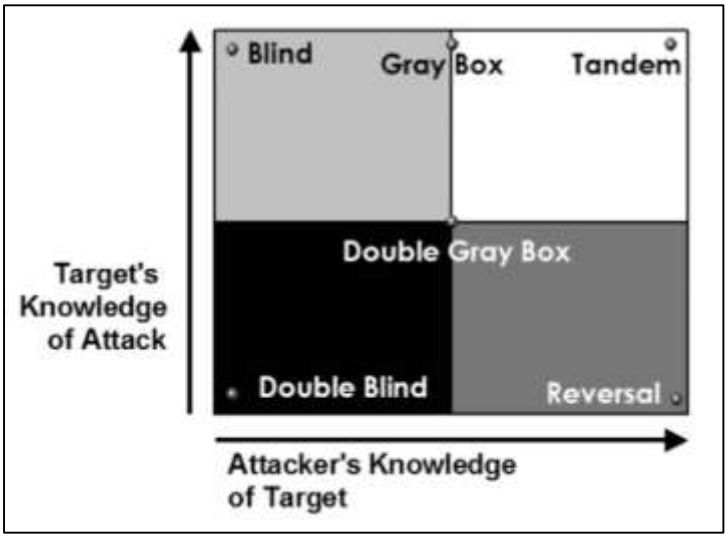



**Figura 1-4:** Tipos de ataques.
**Fuente:** ISECOM, 2017, p.36.

**Tabla 5-4:** Definición de los tipos de ataques.

| **Tipo** | **Descripción** |
|---|---|
| Ciego | El asesor realiza la auditoria de vulnerabilidades de los servidores virtuales, pero sin conocimiento previo de sus defensas, activos o canales. La auditoría ciega es tan amplia dependiendo de las habilidades que posea el asesor probando sus habilidades. Este tipo de prueba también se le conoce como Hacking Ético. |
| Doble persiana | El asesor se compromete con la empresa sin conocimiento previo de sus defensas, activos o canales. En este tipo de auditoria se pone a prueba las habilidades del asesor y los controles que posee la empresa sobre los activos que se tienen en los servidores virtuales. Este tipo de prueba también es conocido como prueba de caja negra o test de penetración. |
| Caja gris | El asesor cuenta con un conocimiento limitado de sus defensas y activos, y con un conocimiento completo de sus canales. El asesor se encuentra preparado para la auditoria conociendo de antemano todos los detalles de la misma. La eficiencia de la prueba depende de la calidad de la información proporcionada y del |

| | |
|---|---|
| | conocimiento del asesor. Este tipo de prueba también es conocida como test de vulnerabilidades y es iniciada por la empresa involucrada para una autoevaluación. |
| Doble caja gris | El asesor se compromete con la empresa con un conocimiento limitado de las defensas y de sus activos, y con un conocimiento completo de sus canales. La empresa notifica por adelantado el alcance y el tiempo que tendrá la auditoria. Este tipo de auditoria tiene la finalidad de poner a prueba las habilidades del asesor y la preparación de la empresa frente a diversos problemas desconocidos que se presenten. La eficiencia de la prueba depende de la calidad de la información proporcionada al analista y de sus habilidades. También es conocido como prueba de caja blanca. |
| Tándem | El asesor conoce todos los detalles que necesita para la auditoria. En la que se prueba la protección y controles que posee la empresa en los servidores virtuales. lo que se prueba aquí son la respuesta de los controles que se tengan frente a problemas no esperados. La eficiencia depende de la calidad de la información proporcionada y de las habilidades que posea el asesor. También se le conoce como una auditoria interna y el asesor forma parte del proceso de seguridad. |
| Reversa | El asesor posee total conocimiento de los controles y seguridad de la empresa, pero la empresa no conoce cuando se realizará la auditoria. La finalidad de esta prueba es ver la respuesta de los controles de la empresa frente a problemas que no conozca en un tiempo desconocido. La eficiencia depende de la calidad de la información proporcionada por la empresa y de las habilidades que posea el asesor. También es conocida como ejercicio de equipo rojo. |

**Fuente:** ISECOM, 2017, p. 37.

**Realizado por:** Arias, Angel; 2019.

### *4.3.3. Arquitectura*

La arquitectura tanto de software como de hardware puede variar dependiendo del servicio que posea el servidor virtual. Las máquinas virtuales sirven como la unidad abstracta de implementación de los servicios que se ofrece y se encuentran acopladas de manera flexible con la arquitectura de almacenamiento en la nube. (Jansen y Grance, 2011, p. 22).

Es importante comprender las tecnologías que utiliza la empresa en los servidores virtuales para ofrecer sus servicios, con lo que la arquitectura se podrá descomponer y mapear en un marco de controles de seguridad y privacidad con la finalidad de evaluar y administrar el riesgo que enfrentan los servidores virtuales. (Jansen y Grance, 2011, p. 22).

#### *4.3.3.1. Ataque a la superficie*

La máquina virtual es una capa adicional de software entre un sistema operativo y una plataforma de hardware. En lo cual el atacante puede tener varios métodos para realizar ataques como son por ejemplo interfaces de programación, sockets (canales), y cadenas de entradas (elementos de datos). (National Institue of Standards and Technology, 2011, p. 22).

Si se desea realizar la paginación, el punto de control y migración de las máquinas virtuales puede existir filtrado de información para que pueda ser utilizado por el atacante. Y un problema que puede presentarse es que maneja varios sistemas operativos a la vez, en el cual por ejemplo con peticiones del protocolo de transferencia de archivos (FTP) puede llegar a corromper el bufer. Teniendo en cuenta tanto la parte virtual como física debe estar correctamente protegida con las políticas de seguridad que posea la empresa. (National Institue of Standards and Technology, 2011, p. 22 - 23).

#### *4.3.3.2. Protección de red virtual*

la mayoría plataformas de virtualización, tienen la capacidad de crear switches basados en softwares y configuraciones de redes lo cual permite que las máquinas virtuales se comuniquen de una manera más rápida y eficiente. El tráfico a través de redes virtuales puede no ser visible para los dispositivos de protección de seguridad en la red física. Para evitar la pérdida de visibilidad y la protección de los ataques contra el host, la duplicación de las capacidades físicas de protección de la red puede ser necesaria en la red virtual. La empresa debe considerar los riesgos y la ventaja de rendimiento de tener el trafico oculto de la red. (National Institue of Standards and Technology, 2011, p. 23).

Un efecto secundario que se puede tener es la posible pérdida de separación de funciones entre roles de administración existentes de la empresa. En el cual los controles son necesarios son muy necesarios para poder mantener seguro los activos que se manejan en los servidores virtuales. (National Institue of Standards and Technology, 2011, p. 23-24).

#### *4.3.3.3. Imágenes de máquinas virtuales*

Los proveedores poseen repositorios con las imágenes de sus sistemas operativos. Una imagen de máquina virtual implica la pila de software, incluida las aplicaciones instaladas y configuradas. Las imágenes de máquinas virtuales que posee la organización deben ser cuidadosamente administradas y controladas para evitar problemas. La empresa debe tratar de mantener actualizadas las máquinas virtuales. (National Institue of Standards and Technology, 2011, p. 24).

La empresa enfrenta riesgos, ya que puede la imagen contener datos y código de propiedad lo cual puede incorporar vulnerabilidades. En donde el atacante puede analizar la imagen para ver si filtra información o le proporciona una vía para el ataque. Otra circunstancia puede ser que el atacante proporcione una imagen para poder de esa manera conseguir los activos de la empresa que desea. (National Institue of Standards and Technology, 2011, p. 24).

#### *4.3.3.4. Protección del lado del cliente*

para que exista una buena seguridad, el cliente también debe encontrarse asegurado. Esto se puede dar ya que la empresa puede solicitar en los diferentes servicios que ofrecen ciertas exigencias mínimas a sus clientes, como puede ser los navegadores entre otras. (National Institue of Standards and Technology, 2011, p. 24).

Pero mantener la seguridad tanto física como lógica de los clientes puede ser muy complicado ya que pueden ingresar desde diferentes dispositivos y si el servicio no se encuentra a su disposición habrá problemas monetarios para la empresa. Los controles en este ámbito a menudo no son tan utilizados o pueden ser eludidos sin ninguna dificultad. (National Institue of Standards and Technology, 2011, p. 24-25).

### 4.4. Métricas de Seguridad

Las métricas de seguridad son variables que se tienen en cuenta para verificar que tan segura es la información de los servicios que se ofrecen en los servidores virtuales, cuando se finaliza correctamente la auditoria, el asesor tiene los datos suficientes de proporcionar métricas precisas sobre el estado de la seguridad. Mientras más eficiente y exhaustiva sea la auditoria, se podrán dar

mejores métricas. Entonces se puede definir a las métricas como la medición de los controles que posee la organización en la cual el asesor a la vez podrá verificar si los datos proporcionados por la empresa son verdaderos o en cuanto han sido manipulados, todo esto dependerá de las habilidades que posea el asesor al momento de realizar la auditoria. Además, una métrica de seguridad adecuada debe evitar los sesgos inherentes a las evaluaciones de los riesgos para asegurar la integridad de las mediciones. Todas estas características se han combinado para crear los ravs, lo cual es una descripción objetiva e imparcial de un ataque de superficie. (ISECOM, 2017, p. 62 - 63).

### *4.4.1. Que son los ravs*

El rav es una medida de ataque de la superficie, es la cantidad de interacciones no controladas con la empresa, la cual se calcula mediante el equilibrio cuantitativo entre operaciones, limitaciones y controles. En la escala, se considera que tener 100 ravs es el equilibrio perfecto, en lo cual si se tiene una menor cantidad de ravs quiere decir que no se tiene mucha seguridad. En cambio, que más de 100 ravs muestra que la empresa posee más de los controles necesarios, lo cual puede ser un problema ya que se tendría más interacciones de las requeridas, agregando a la par problemas de complejidad y mantenimiento. (ISECOM, 2017, p. 64)

El rav no mide la superficie de un ataque, sino que permite su medición. No puede decir si un objetivo en particular será atacado, sino que informa donde atacaran, contra que tipos de ataques se puede defender con éxito y que daño puede llegar a causar el atacante. Con lo cual será más fácil analizar los riesgos que se tengan de una manera mucho más precisa. (ISECOM, 2017, p. 64).

El rav son varios cálculos por separado en los que se toman en cuenta la porosidad, controles y limitaciones, en el cual se combinan todas mostraran el tamaño de la superficie de ataque de una manera práctica. (ISECOM, 2017, p. 64) De acuerdo a ISECOM (2017), en las cuales las dos formas son:

- **Cálculo directo:** es el cálculo delta, es muy eficiente para conocer como un nuevo individuo, proceso o control cambiara la seguridad que se tiene en la empresa. En la cual el rav puede ser positivo o negativo, en el cual muestra que tan lejos se encuentra la empresa de un balance de seguridad perfecto. Delta positivo es un indicador que muestra que se gasta demasiado en los controles o si el gasto es excesivo en algún tipo de control. Delta negativo muestra una falta de controles o que algún control no posee los recursos necesarios para proteger los activos que manejan los servidores virtuales de una manera adecuada. Pero el rav tiene un mejor desempeño en la segunda manera.

- **Seguridad real:** sirve para poder comprender un panorama general. El delta se basa en un equilibrio perfecto, pero también controles adicionales y redundantes para poder producir una métrica más amigable y familiar. En el cual el rav se calcula con un logaritmo de base 10. El equilibrio perfecto se estable en 100 y los cálculos se realizan con respecto a cómo varia ese valor. Lo cual permitirá al asesor y a la empresa de tener una visión rápida y fácil de todos los objetivos.

De acuerdo a ISECOM (2017), el verdadero poder del rav es como puede proporcionar respuestas a las siguientes ocho preguntas de seguridad fundamental con gran precisión:

- ¿Cuánto dinero debe gastar la empresa en seguridad?

El rav puede mostrar la cantidad actual de seguridad que se tiene, con lo cual se pueden hacer proyecciones y definir los controles y parámetros antes de que se realice o se implemente una solución. Dependiendo de las proyecciones que se realicen y de los controles y parámetros que se deseen implementar, con ello definir un precio para la realización de las soluciones. En el que se tratara de tener un perfecto balance con respecto a los ravs. (ISECOM, 2017, p. 65)

- ¿Qué se debe proteger primero?

Con la utilización del rav se puede ver el auditoria de vulnerabilidades de los servidores virtuales como una gran pintura, en la que se presentaran todos los problemas que se tengan. Después, el rav puede mostrar cual es el punto que tiene más porosidad y con ella que necesita mayores controles. Con lo que se desea proteger, se evaluara y se definirá el activo que se maneje que más se desea proteger. (ISECOM, 2017, p. 65).

- ¿Qué soluciones de protección necesitamos y como configurarla para obtener la máxima eficiencia?

Un estudio completo del rav, muestra los 10 controles que se tiene y las limitaciones de dichos controles. Después el asesor puede seleccionar las soluciones basadas en los controles que se escogieron. Cuando se escogen los controles para la implementación, se deben utilizar en las áreas que los controles que se utilizan tengan mayor deficiencia. (ISECOM, 2017, p. 65).

- ¿Cuánta mejora se obtiene mediante adquisiciones y procesos de seguridad específicos?

Una ventaja del rav es que se puede ver qué soluciones se piensa aplicar, comparándolas con otras soluciones. Combinando con el análisis que se realiza de la red y a la par con el rav se puede definir el lugar más apropiado para realizar las soluciones y controles que el asesor vea pertinente. A la vez

que es de gran ayuda ya que permite predecir el valor que se tendrá de protección. (ISECOM, 2017, p. 65).

- ¿Cómo medir los esfuerzos y mejoras periódicas de seguridad?

Una ventaja que el rav presenta es la de poder comparar los valores actuales con los antiguos valores. Lo cual permitirá que los cambios que se realicen y el precio que se tengan se encuentren completamente justificados. (ISECOM, 2017, p. 66).

- ¿Cómo sabemos si reducimos la exposición de activos a las amenazas?

Con el conocimiento de los controles que se tiene, se puede conocer cuál es el punto que sufre más amenazas. En el rav una amenaza puede aparecer en donde se tengan interacciones, pero no controles. Con el análisis de la red se puede determinar los riesgos y en donde aplicar los controles según el asesor determine necesario, y con ello proteger los activos que se manejen en los servidores virtuales. (ISECOM, 2017, p. 66).

- ¿Puede el rav informarnos como resistir los ataques?

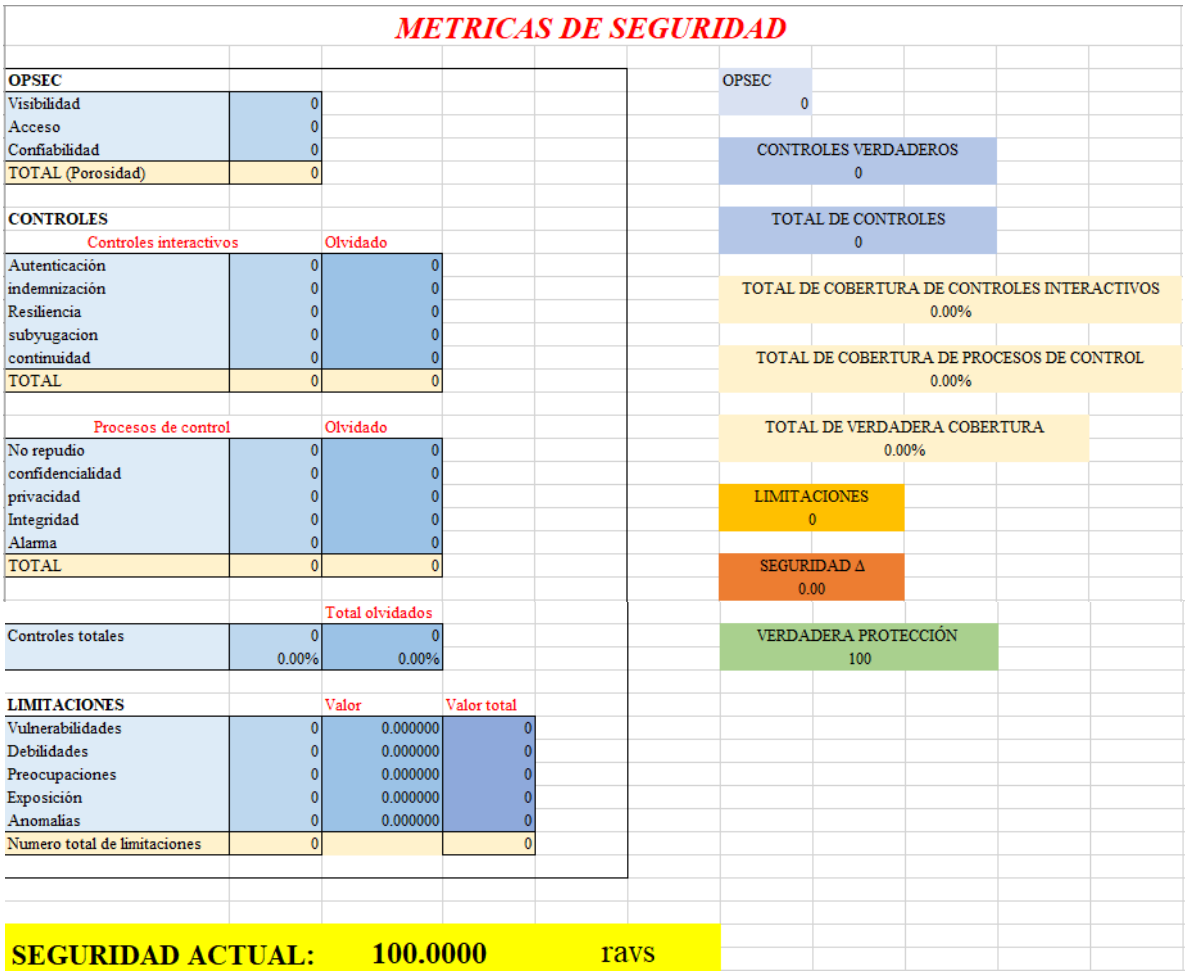
Si, ya que se puede balancear las interacciones con los controles que se tengan. Según el ataque que se tenga se puede prevenir o mitigar con los controles que se hayan implementado. (ISECOM, 2017, p. 66).

- ¿Puede el rav ayudar con el cumplimiento normativo?

El rav puede ayudar al asesor a realizar un buen trabajo, manteniendo seguro los activos que se tengan con los controles preestablecidos o que se vean necesarios su implementación. El puntaje del rav puede ayudar a conocer varios requerimientos que se necesiten. (ISECOM, 2017, p. 66).

### *4.4.2. Como hacer un rav*

El rav necesita un análisis en orden, para poder contar las cosas correctamente y realizar un análisis verdadero. El rav fue originalmente desarrollando para análisis, el auditor toma más en cuenta el comportamiento del atacante respecto a los activos que se manejen en vez de la configuración. Si el rav se aplica a análisis no operacionales, se puede determinar el nivel de seguridad del software y su complejidad, o en la seguridad física se puede hacer una lista para verificar y determinar los niveles de protección físico que se proveen. (ISECOM, 2017, p. 67).



**METRICAS DE SEGURIDAD**

| OPSEC | |
|---|---|
| Visibilidad | 0 |
| Acceso | 0 |
| Confiabilidad | 0 |
| TOTAL (Porosidad) | 0 |

| CONTROLES | | |
|---|---|---|
| Controles interactivos | | Olvidado |
| Autenticación | 0 | 0 |
| indemnización | 0 | 0 |
| Resiliencia | 0 | 0 |
| subyugacion | 0 | 0 |
| continuidad | 0 | 0 |
| TOTAL | 0 | 0 |

| | | |
|---|---|---|
| Procesos de control | | Olvidado |
| No repudio | 0 | 0 |
| confidencialidad | 0 | 0 |
| privacidad | 0 | 0 |
| Integridad | 0 | 0 |
| Alarma | 0 | 0 |
| TOTAL | 0 | 0 |

| | | |
|---|---|---|
| | | Total olvidados |
| Controles totales | 0 | 0 |
| | 0.00% | 0.00% |

| LIMITACIONES | | Valor | Valor total |
|---|---|---|---|
| Vulnerabilidades | 0 | 0.000000 | 0 |
| Debilidades | 0 | 0.000000 | 0 |
| Preocupaciones | 0 | 0.000000 | 0 |
| Exposición | 0 | 0.000000 | 0 |
| Anomalías | 0 | 0.000000 | 0 |
| Numero total de limitaciones | 0 | | 0 |

| | |
|---|---|
| OPSEC | 0 |
| CONTROLES VERDADEROS | 0 |
| TOTAL DE CONTROLES | 0 |
| TOTAL DE COBERTURA DE CONTROLES INTERACTIVOS | 0.00% |
| TOTAL DE COBERTURA DE PROCESOS DE CONTROL | 0.00% |
| TOTAL DE VERDADERA COBERTURA | 0.00% |
| LIMITACIONES | 0 |
| SEGURIDAD Δ | 0.00 |
| VERDADERA PROTECCIÓN | 100 |

**SEGURIDAD ACTUAL: 100.0000 ravs**

**Figura 2-4:** Metricas de seguridad para ámbito real.

**Realizado por:** Arias, Angel; 2019.

El menor de los ravs se puede calcular con la porosidad en la que se tienen huecos en su alcance. Los problemas con las métricas de seguridad es que el asesor pueda determinar que el realmente no sabe. En el rav dicho problema no existe, en el que se conoce con un particular vector y no se realizan especulaciones. En el que se puede contar y verificar todas las interacciones que sean visibles, y a la vez las interacciones que se encuentren fueran del alcance. La porosidad toma en cuenta tres parámetros para el valor del rav final. La primera parte que el rav toma en cuenta es la visibilidad, el acceso y la confiabilidad. La segunda parte que se toman en cuenta los diez controles tanto los controles interactivos como los procesos de control. Cada parámetro que compone cada uno de los controles tiene un valor del 10%, en la que ayudara a prevenir todo tipo de ataques. Esto es gracias a que los diez controles que se tienen en cuenta no tienen limitaciones. Y la tercera parte que el rav utiliza son las limitaciones que se encuentran en la protección y controles, en las que se toman en

cuenta la exposición, vulnerabilidades, debilidades, preocupación y anomalías. (ISECOM, 2017, p. 67-68).

## 4.5. Seguridad Wireless

El presente canal comprende las redes desde las cuales acceden los diferentes usuarios a los servicios que se tengan en los servidores virtuales. el objetivo es el de verificar o comprobar que se tenga una seguridad estándar dentro o fuera de la empresa. En la cual el analista el momento que realice la auditoria no debe invadir la vida privada de las personas, tales como, grabar o escuchar conversaciones personales. (ISECOM, 2017, p. 138).

### *4.5.1. Verificación de detección activa*

De acuerdo a ISECOM (2017), en el presente punto el asesor puede realizar varias actividades para mantener seguro los activos de los servidores virtuales como son:

- **Monitoreo del canal:** test que verifica que los controles se encuentran implementados para monitorear las amenazas.
- **Moderación del canal:** test que verifica que los controles se encuentran implementados para mitigar las amenazas, o alertar de acciones por personas no autorizadas. (ISECOM, 2017, p. 138).

### *4.5.2. Auditoria de visibilidad*

El asesor analiza la visibilidad que tengan los usuarios, y que no posean privilegios que no les correspondan, es decir, no puede poseer los mismos privilegios un usuario común en comparación a un administrativo. (ISECOM, 2017, p. 141) De acuerdo a ISECOM (2017), para ello se toma en cuenta los siguientes puntos:

- Test para analizar las interacciones que se tengan
- Recolectar información y el número de peticiones para que no exista problemas con los servicios de los servidores virtuales.

### *4.5.3. Acceso a los servicios de los servidores virtuales*

El asesor debe analizar los diferentes tipos de redes desde las cuales los usuarios pueden ingresar, en las que se toman en cuenta: red privada (Modem de casa), red empresarial, datos móviles y red pública. Y se verifica las limitaciones que se tienen o que se pueden dar en los diferentes tipos de redes. (ISECOM, 2017, p. 142).

### *4.5.4. Controles*

De los controles mencionados en el capítulo 1. De acuerdo a ISECOM (2017), se toman en cuenta los siguientes puntos tanto de los controles interactivos como de los procesos de control:

- **No repudio:** el asesor verifica si se realiza alguna acción indebida por personas no autorizadas, el atacante no pueda negar las acciones realizadas.
- **Resiliencia:** asegurar que cuando se tengan interacciones desde redes externas a la de la empresa, no exista fuga de la información.
- **Subyugación:** verificar que todas las interacciones que se realicen desde los diferentes tipos de redes se encuentren dentro de los parámetros de seguridad establecidos.
- **Continuidad:** verificar que los diferentes usuarios tengan acceso a los servicios que se tengan en los servidores virtuales.
- **Alarma:** que se active o notifique una alarma en el caso de que un usuario de la misma o de diferente red realice acciones no autorizadas. (ISECOM, 2017, p. 142-144)

### *4.5.5. Verificación de las configuraciones*

Es un test que se realiza para evitar la seguridad que se tengan en los servidores virtuales. (ISECOM, 2017, p. 145) De acuerdo a ISECOM (2017) para ello se toman en cuenta algunos puntos como son:

- **Errores comunes de configuración:** realiza pruebas como de denegación de servicio para los servicios de los servidores virtuales, verificar si sufren ese tipo de ataques.
- **Configuración de controles:** se examinan los controles que se tengan o implementaron de acuerdo a la información que se desea proteger.

- **Evaluación de las configuraciones:** se verifica los controles que se mejoraron o los controles nuevos implementados que el asesor vea oportuno.

## 4.6. Análisis de la seguridad de la red de datos

Para poder comprobar que se tiene seguridad en la red de datos, debe existir interacciones entre el atacante y los activos que se manejan en los servidores virtuales. también es conocido como pruebas de seguridad, el cual su objetivo es de poder comprobar y verificar como se encuentran los controles y que grado de seguridad se tiene en la empresa frente a específicos ataques según sea el activo que se esté manejando. El asesor debe tener total confidencialidad con la empresa para que no exista ningún filtrado de información con alguna empresa que sea competencia, en el caso de que el análisis de ataques sea exitoso. (ISECOM, 2017, p. 167)

Las pruebas deben ser dirigidas hacia los sistemas de los servidores virtuales a la que se le está realizando la auditoria, tomando en cuenta el alcance que se tendrá en el momento de la auditoria y la confidencialidad con la empresa para que no exista ningún problema en el futuro. La información personal de los trabajadores debe continuar siendo privada. (ISECOM, 2017, p. 167)

### *4.6.1. Logística*

En el presente punto se realizan las pruebas de canal necesario para asegurar que los resultados encontrados serán positivos o negativos. (ISECOM, 2017, p. 169) De acuerdo a ISECOM (2017), se toman en cuenta los siguientes puntos:

#### *4.6.1.1. Framework*

- Verificar el alcance para la auditoria.
- Verificar las direcciones IP que proporcionan acceso para poder configurar los servicios de los servidores virtuales
- Buscar nombres de dominios parecidos o que se puedan confundir con la dirección del servicio del servidor virtual. (ISECOM, 2017, p. 169)

*4.6.1.2. Calidad de la red*

- Mida la tasa de peticiones en UDP, TCP e ICMP. El paquete se transporta en UDP cuando se requiere grandes interacciones como videoconferencia, TCP cuando se acceden a páginas informativas e ICMP cuando se realiza ping.
- Registrar porcentajes de pérdidas de paquetes para el envío y recepción determinada. (ISECOM, 2017, p. 169)

### *4.6.2. Verificación de detección activa*

El filtrado de los datos que se van a analizar para verificar s existen ataques se deben realizar antes de la respectiva mitigación. (ISECOM, 2017, p. 170) De acuerdo a ISECOM (2017), se puede tener en cuenta los siguientes puntos para tener un punto de partida:

- Comprobar los tiempos de respuestas cuando se acceden a los servicios que poseen los servidores virtuales como pueden ser páginas web informativas.
- Verifique las respuestas activas, esto puede ser una alarma que salte en el caso de que exista algún problema.
- Asignar cualquier aplicación, sistema o segmento de red para que salte cuando se tenga alguna alarma, notificación o registros. En el cual se podría incluir algún tipo de ataque que sufran los servicios de los servidores virtuales. (ISECOM, 2017, p. 170)

### *4.6.3. Visibilidad de la auditoria*

En este punto se establecen los objetivos que se desean cumplir. (ISECOM, 2017, p. 171) De acuerdo a ISECOM (2017), se toma en cuenta los siguientes puntos:

- Identificar que se analizara en la red.
- Consultar los servidores y sistemas operativos que se tengan, así como los servicios que se tengan en los servidores virtuales.
- Verificar las solicitudes y las respuestas que se tengan.
- Verificar las respuestas para seleccionar los puertos para analizar. Por ejemplo: TCP 8, 22, 23, 25, 80, 443, 445, 1433.

- Rastrear la ruta de los paquetes TCP.
- Examinar los servicios y aplicaciones que se tengan en los servidores virtuales. para verificar que no se muestre información adicional, se puede analizar, por ejemplo: http, dns, mysql, etc.
- Verificar las respuestas que se tengan a las peticiones TCP SYN.
- Verificar las respuestas de las solicitudes de servicio TCP a los puertos.
- Verificar las respuestas de un TCP ACK con puerto 80 como salida.
- Verificar las respuestas de los fragmentos de las peticiones TCP SYN.
- Verificar las combinaciones de todas las respuestas de TCP. (ISECOM, 2017, p. 171)

### *4.6.4. Verificación de acceso*

Se verifican los puntos de acceso para el análisis. (ISECOM, 2017, p. 173) De acuerdo a ISECOM (2017), se toman en cuenta los siguientes puntos:

- Hacer coincidir cada puerto abierto con un servicio, aplicación y/o protocolo.
- Verificar el tiempo de respuestas con respecto a con las ultimas vulnerabilidades y parches.
- Verificar la aplicación que se tiene en los servidores virtuales y la versión.
- Verificar HTTP y HTTPS para el alojamiento virtual. (ISECOM, 2017, p. 173)

### *4.6.5. Confianza de verificación*

Pruebas que se realizan para verificar que la información que se esté proporcionando en los servicios de los servidores virtuales son verdaderos. (ISECOM, 2017, p. 174) De acuerdo a ISECOM (2017), se toman en cuenta los siguientes puntos:

- Verificar los URL de los servicios que se tengan en los servidores virtuales.
- Verificar que no se pueda duplicar la página web.
- Examinar los registros de dominio.
- Verificar que los usuarios que ingresen sean a los servicios correctos. (ISECOM, 2017, p. 174).

### *4.6.6. Controles de verificación*

Para los servicios de los servidores virtuales se toman en cuenta principalmente la confidencialidad y la integridad. (ISECOM, 2017, p. 175) De acuerdo a ISECOM (2017), se pueden tomar en cuenta los siguientes puntos:

- Verificar que no exista ningún filtrado de información que no sea la que no se desea mostrar.
- Probar la encriptación que posean los servicios de los servidores virtuales para que no sean modificados por una persona no autorizada.
- Verificar que pueden visualizar los usuarios externos.
- Verificar que la información mostrada sea la verdadera. (ISECOM, 2017, p. 175)

### *4.6.7. Proceso de verificación*

En esta fase se realizan pruebas para verificar los controles que se han realizado para mitigar las vulnerabilidades. (ISECOM, 2017, p. 176) De acuerdo a ISECOM (2017), se toman en cuenta los siguientes puntos:

- Examinar y documentar el alcance que tienen los servicios de los servidores virtuales, notificaciones y respuestas de las alarmas frente a problemas que se presenten.
- Verificar el nivel de incidentes que se presenten y el tiempo de respuesta.
- Determinar hasta qué punto las alarmas y notificaciones se pueden ampliar y/o modificar.
- Documentar y enumerar los objetivos que se encuentran protegidos contra diferentes tipos de ataques. (ISECOM, 2017, p. 176).

### *4.6.8. Verificación de las configuraciones*

En esta fase se realizan todas las pruebas necesarias para recopilar la información, como se pretende que funciones los diferentes controles que se han implementado. (ISECOM, 2017, p. 177) De acuerdo a ISECOM (2017), se toman en cuenta los siguientes puntos para poder realizarlo:

- Examinar los controles que se tengan y que cumpla con su respectiva función manteniendo seguro los activos de los servicios de los servidores virtuales.

- Examinar la lista de control de acceso (ACL) para que personas no autorizadas no puedan modificar los activos.
- Verificar que los controles implementados no sean redundantes
- Verificar que las configuraciones predeterminadas que se tengan de los servicios sean modificadas para poder asegurar los activos que se manejen en los servidores virtuales.
- Verificar que la administración y los cambios que se realicen como puede ser en páginas web informativas solo lo puedan realizar el personal autorizado.
- Verificar que no exista servicios que no sean utilizados. (ISECOM, 2017, p. 177).

## 4.7. Pruebas de Penetración

### *4.7.1. Aplicaciones del servidor*

El descubrimiento de aplicaciones web es un proceso con la finalidad de encontrar aplicaciones web en una empresa o infraestructura especifica. Se suele entregar un conjunto de direcciones IP o en un conjunto de DNS, esta información se entrega antes de la realización de una prueba de análisis de vulnerabilidades o de una prueba de penetración. Hay tres factores que influyen en cuanto a las aplicaciones se encuentran relacionadas a un determinado DNS o dirección IP: (OWASP, 2017, p. 50).

#### *4.7.1.1. URL con bases diferentes*

El punto de entrada a una aplicación web es por lo general www.ejemplo.com o la dirección IP por ejemplo 192.168.1.100. Si la pagina dispone de servicios adicionales puede estar asociados a diferentes aplicaciones web, por ejemplo: www.ejemplo.com/url1 www.ejemplo.com/url2. (OWASP, 2017, p. 50).

En primer lugar, si el servidor esta mal configurado y permite navegar por el directorio, es posible detectar aplicaciones. Una ayuda en este sentido son los escáneres de vulnerabilidades. Un escáner de vulnerabilidades que analiza las mayores vulnerabilidades es OWASP ZAP de licenciamiento libre (OWASP, 2017, p. 50).

En segundo lugar, puede que las paginas conduzcan a una pagina falsa que no es la real o que reenvíen a otras paginas. Los evaluadores pueden analizar los sitios web, en el cual se puede encontrar URLs que se encuentren apuntando a otras aplicaciones. (OWASP, 2017, p. 50 – 51).

#### *4.7.1.2. Puertos no-estándar*

Las aplicaciones web generalmente se ubican en los puertos 80 (Http) y 443 (Https), dependiendo la aplicación web a la que se ingrese puede tener un numero de puerto arbitrario, los mismos que pueden ser referenciados como a continuación: www.ejemplo.com:puerto

Un escáner de puerto que se puede utilizar es nmap, el cual es capaz de realizar varias opciones según sean necesarias en el cual se obtendrán varios parámetros como son:

- El puerto que contiene el servidor.
- Si el puerto se encuentra abierto o cerrado.
- Los paquetes que envían mediante ese puerto.
- La versión del sistema en el que es utilizado.

#### *4.7.1.3. Hospedajes virtuales*

Una dirección IP única asociada, por ejemplo: la dirección IP 192.168.1.100 se puede asociar a un servicio web como puede ser www.ejemplo.com. En el cual se puede realizar la relación de 1 a N en el cual se puede usar diferentes contenidos denominados hospedajes (host) virtuales. (OWASP, 2017, p. 50)

De acuerdo a OWASP (2017), hay una serie de técnicas la dirección IP que se encuentra asociada al DNS:

- Transferencia de zona DNS
- Consulta inversa de DNS
- Búsquedas DNS basadas en la web
- Servicios de IP inversa

Teniendo identificado las vulnerabilidades que tiene el servicio web que se esta analizando gracias a la aplicación OWAS ZAP, que toma en cuenta el Top Ten de Owasp los cuales son:

### *4.7.2. SQL Inyección*

Casi cualquier vector puede ser víctima de un ataque de SQL inyección, los cuales ocurren cuando un atacante puede enviar información dañina. Las vulnerabilidades de inyección se encuentran muy a menudo en las consultas SQL, NoSQL, LDAP, XPath, comandos del Sistema Operativo, analizadores XML, encabezados SMTP, lenguajes de expresión, parámetros y consultas ORM. (OWASP Top 10, 2017, p. 7)

Los errores de inyección son fáciles de descubrir cuando se analiza el código, así como los escáneres ayudan a encontrarlos. Para la empresa es muy importante no tener este tipo de vulnerabilidades ya que puede causar perdida, divulgación y/o corrupción de la información, perdida de auditabilidad o denegación de acceso. El impacto que se genera en la empresa si se sufre este tipo de ataques depende de las necesidades de la aplicación web y de los datos. (OWASP Top 10, 2017, p. 7)

De acuerdo a OWASP Top 10 – 2017, se sabe que la aplicación web es vulnerable a este tipo de ataques cuando:

- Los datos que son ingresados por el usuario no son validados, filtrados o analizados por la aplicación.
- Se realizan consultas dinámicas o no parametrizadas, sin codificar los parámetros de forma acorde al contexto.
- Se utilizan datos o secuencia de comandos dañinos para poder extraer registros adicionales que sean sensibles para la empresa sin que se den cuenta.
- Cuando los datos dañinos se usan directamente o se concatenan, de modo que contiene datos y estructuras para que se vuelva una consulta dinámica, comandos o procedimientos almacenados. (OWASP Top 10, 2017, p. 7)

El concepto de la realización del ataque de inyección es idéntico entre todos los tipos de consultas. La revisión del código fuente es el mejor método para detectar si las aplicaciones web son vulnerables a ataques de inyección, seguido de cerca por diferentes tipos de pruebas de todos los parámetros, encabezados, URL, cookies, JSON, SOAP y entradas de datos XML. (OWASP Top 10, 2017, p. 7)

En las pruebas se deben incluir pruebas de ataques de inyección tanto dinámicas (DAST) como estáticas (SAST), para identificar de la mejor manera los errores que se tengan respecto a este tipo de ataque. (OWASP Top 10, 2017, p. 7)

De acuerdo a OWASP Top 10 – 2017, Para prevenir este tipo de ataques se puede tomar en cuenta los siguientes puntos:

- Separar los datos de los comandos y las consultas.
- Utilizar un API seguro, que evite el uso de un intérprete por completo y proporcione una interfaz parametrizada. Icluso cuando se parametrizan las peticiones o consultas puede existir ataques de inyección si es que permite concatenar datos y consultas.
- Realizar validaciones de entradas de datos en el servidor con la utilización de listas blancas. Pero no es una defensa completa ya que muchas aplicaciones cuando se realiza una consulta o petición requiere el uso de caracteres especiales como puede ser en: campos de textos, APIs o aplicaciones móviles.
- Cuando se realice una consulta dinámica, tratar de omitir lo máximo posible el ingreso de caracteres especiales utilizando la sintaxis de caracteres específicos para el usuario del que se trate. La estructura en SQL como se tiene el nombre de las tablas, nombre de las columnas, entre otras. No se pueden escapar, por lo tanto, los nombres suministrados por el usuario son peligrosos.
- Utilizar Limit y otros controles de SQL para que en el caso no deseado sucede un ataque de inyección se evite la fuga masiva de registros. (OWASP Top 10, 2017, p. 7)

### *4.7.3. Perdida de autenticación*

Los atacantes tienen acceso tanto a las claves como a los usuarios conocidos debido a la fuga de la información, además de cuentas administrativas por defecto. Este tipo de ataque para la realización muy comúnmente se utilizan ataques de fuerza bruta o la utilización de diccionarios para descubrir las contraseñas. (OWASP Top 10, 2017, p. 8).

Las pérdidas de autenticación son muy comunes y esto se debe al diseño y la implementación de la mayoría de los controles de acceso. En donde siempre se tiene presente la gestión de sesiones para los controles de autenticación y se encuentra presente en las aplicaciones web que solicitan al cliente un usuario y contraseña. (OWASP Top 10, 2017, p. 8).

Los atacantes para comprometer a todo el sistema solo deben obtener el acceso a algunas cuentas o a una sola cuenta de una persona administrativa. Dependiendo el acceso que disponga cada persona esto puede generar a la empresa el robo de identidad, lavado de dinero y la divulgación de la información sensible de la empresa. (OWASP Top 10, 2017, p. 8).

De acuerdo a OWASP Top 10 – 2017, La aplicación web puede tener vulnerabilidades a este tipo de ataques si:

- Permite la reutilización de credenciales conocidas en ataques automatizados, cuando el atacante ha obtenido los datos de algunos usuarios y claves válidos.
- Permite ataques de fuerza bruta y/o ataques automatizados.
- Permite que los usuarios que utilizan la aplicación web el uso de contraseñas por defecto, débiles o muy conocidas.
- Posee procesos débiles o que no son eficientes cuando en el proceso de desea la recuperación de credenciales.
- Almacena las contraseñas en texto plano es decir sin codificarlas, o si se codifican las claves la codificación es muy débil.
- No posee autenticación multifactor, es decir, que es un sistema que no tiene más de una forma para verificar la legitimidad del usuario o fue implementada de una forma ineficaz.
- Expone sesiones que fueron realizadas en la URL, no las invalida correctamente o no rota de una forma satisfactoria luego del cierre de sesión o de un periodo determinado por la empresa. (OWASP Top 10, 2017, p. 8).

Para poder prevenir este tipo de ataques y asegurar los usuarios y contraseñas de los clientes, se puede tener en cuenta los siguientes puntos:

- Utilizar la autenticación multifactor, es decir, que el usuario el rato que desee ingresar o realizar alguna acción, pida más de una forma para verificar que es el usuario verdadero, y así tratar a la vez de mitigar los ataques de fuerza bruta, ataques automatizados o la reutilización de credenciales robadas.
- No utilizar credenciales por defectos principalmente si es una persona administrativa.
- Implementar controles para que los clientes no utilicen contraseñas débiles. Las contraseñas débiles más comunes se pueden consultar en: https://github.com/danielmiessler/SecLists/tree/master/Passwords.
- Asegurarse que el registro, la recuperación de credenciales y el uso de APIs, no permitan ataques de enumeración de usuarios, en el cual el atacante trata de obtener un listado de los usuarios en la plataforma.
- Limitar y/o incrementar el tiempo de respuesta de cada intento fallido de inicio de sesión. Registrar todos los fallos y avisar a los administrativos cuando se detecte un ataque de fuerza bruta.
- La ID de la sesión no se debe incluir en la URL de la aplicación web, debe ser almacenado de una forma segura e invalidado posteriormente del cierre de la sesión, mediante la utilización de

un gestor de sesiones en el servidor, integrado, seguro y que genere un nuevo ID de sesión aleatorio. (OWASP Top 10, 2017, p. 8).

A continuación, se puede observar ejemplos de escenarios en los que se pueden tener este tipo de ataques:

- El relleno automático de las credenciales y el uso de una lista de contraseñas conocidas.
- Cuando en la empresa tiene como único factor de inicio de sesión o de la realización de alguna acción solo la contraseña y no algo adicional para asegurar que el cliente que se encuentra realizando dicha acción es el auténtico.
- El número de intentos que puede realizar el usuario es indefinido es decir que puede intentar las veces que desee el ingreso a una aplicación como cierto usuario.

### *4.7.4. Exposición de datos sensibles*

En lugar de atacar la criptografía de la aplicación web, los atacantes roban claves, datos de texto plano del servidor en tránsito o desde el cliente mediante la realización del ataque de man in the middle el cual consiste en la recepción de todos los datos que se envíen entre el cliente y el servidor y poder desencriptarlo para conocerlos. (OWASP Top 10, 2017, p. 9).

En los últimos años este tipo de ataques han sido los que han tenido un mayor impacto porque las empresas no se encargan de encriptar correctamente la información sensible. En el cual cuando se utiliza la criptografía es muy común la generación y gestión de claves, algoritmos, cifrados y protocolos débiles. Para los datos que se encuentran en tránsito las debilidades son muy fáciles de detectar que mientras para los datos que se encuentran almacenados son muy difíciles, en la cual ambos casos tienen una forma de explotarlos muy variable. (OWASP Top 10, 2017, p. 9).

Cuando se genera este tipo de ataques se comprometen los datos que deberían estar correctamente protegidos en donde se toma en cuenta la información personal sensible como los registros de salud, datos personales, credenciales y la información de las tarjetas de créditos de los clientes que requieren una mayor protección. (OWASP Top 10, 2017, p. 9).

Para saber si la aplicación es vulnerable a este tipo de ataques en primer lugar se debe tener en cuenta el tipo de información que la empresa considera más importante y a cuál se va a dar una mayor relevancia para protegerla. Para esto según OWASP Top 10 – 2017 se toma en cuenta:

- Se transmiten los datos en texto plano es decir sin la correcta codificación que se requiere o sin ser codificados siendo información sensible. A la vez verificar el tráfico interno, por ejemplo: los balanceadores de carga, los servidores web, entre otras.
- La utilización de código de codificación muy débiles, que sea por defecto o que sean heredados.
- Utilización de claves criptográficas predeterminadas, utilización de claves débiles o una incorrecta gestión de la rotación de las claves. (OWASP Top 10, 2017, p. 9).

Para la mitigación de este tipo de ataques se dan los siguientes consejos:

- Identificar qué información es sensible de cada uno de los clientes y dar la seguridad que la empresa considere oportuna para cada dato.
- Aplicar los controles adecuados según la empresa.
- No almacenar datos sensibles que no son utilizados, ya que pueden ser robados y no tiene ninguna finalidad tener dicha información.
- Cifrar todos los datos sensibles cuando sean almacenados.
- Cifre todos los datos en tránsito utilizando cifrados fuertes o en los que se tenga bastante confianza de no poder ser descifrados.
- No crear propios algoritmos de cifrados sino utilizar protocolos y estándares que sean fuertes con una gestión adecuada de claves.
- Deshabilitar el almacenamiento en el cache de los datos sensibles.
- Verificar la eficiencia de las configuraciones y de los parámetros de una forma independiente. (OWASP Top 10, 2017, p. 9).

A continuación, se explica unos ejemplos en los que pueden suceder este tipo de ataques:

- Cuando una aplicación web cifra números de tarjetas de crédito de manera automática, puede existir un ataque de inyección SQL y el atacante puede obtener los números de la tarjeta en texto plano es decir sin codificación.
- Cuando no se usa un cifrado cuando se transmiten los datos en una aplicación web, el atacante puede analizar el tráfico de la misma y descubrir los diferentes datos que el usuario ingrese y a la vez puede secuestrar la sesión del usuario. (OWASP Top 10, 2017, p. 9).

### *4.7.5. Entidades externas XML*

Si los procesadores XML si cargan o incluyen contenido hostil en un documento XML, el atacante puede explotar el código que sea vulnerable, sus dependencias o integraciones que posea la aplicación web. (OWASP Top 10, 2017, p. 10).

Muchos procesadores XML antiguos permiten la especificación de una entidad externa, las herramientas que analizan el código desde su origen pueden encontrar estos problemas analizando las dependencias y configuraciones. Los atacantes realizan este tipo de ataques con la finalidad de extraer datos, ejecutar una solicitud remota desde el servidor, escanear sistemas operativos internos de la empresa, realizar ataques de denegación de servicio y ejecutar otro tipo de ataques. (OWASP Top 10, 2017, p. 10).

Según OWASP Top 10 – 2017, las aplicaciones que son basados en XML o integraciones son vulnerables si:

- La aplicación acepta y carga XML desde fuentes no confiables o hace la inserción de datos no confiables en documentos XML. Estos datos deben ser analizados sintácticamente por un procesador XML.
- La aplicación utiliza un estándar abierto para intercambiar la información de autorización y autenticación para el procesamiento de identidades, utiliza XML para garantizar la identidad de los usuarios y puede ser vulnerable.
- Si la aplicación es vulnerable a este tipo de ataques es muy probable que también lo sea frente a ataques de denegación de servicio. (OWASP Top 10, 2017, p. 10).

Para poder prevenir este tipo de ataques, según OWASP Top 10 – 2017, se requiere:

- Utilización de datos menos complejos como JSON, joomla y evitar la serialización de datos confidenciales.
- Tener actualizados todos los requerimientos como bibliotecas y procesadores XML que utiliza la aplicación web o el sistema adyacente.
- Deshabilitar las entidades externas de XML.
- Implementación de una lista blanca, es decir, entradas positivas al servidor para poder evitar el ingreso de datos dañinos dentro de documentos, cabeceras y nodos XML.
- Si estos controles no son posibles considerar la utilización de un parche virtual, firewalls para detectar, monitorear y bloquear este tipo de ataques. (OWASP Top 10, 2017, p. 10).

### *4.7.5. Pérdida de control de acceso*

La explotación del control de acceso es una habilidad esencial de los atacantes. Los analizadores de vulnerabilidades pueden detectar la ausencia de controles de acceso, pero no pueden verificar si son correctos. Es detectable mediante medios manuales o de forma automática en algunos frameworks que carecen de controles de acceso. (OWASP Top 10, 2017, p. 11).

Este tipo de ataques son muy comunes debido a la falta de detección automática y a la falta de pruebas efectivas por parte de los desarrolladores de aplicaciones. Este tipo de ataque no suele ser cubierto por pruebas automatizadas, ni en estático como en dinámico. (OWASP Top 10, 2017, p. 11).

El ataque de forma anónima corresponde a atacantes que se hacen pasar por clientes o administrativos de la empresa, en la cual se encargan de utilizar funciones privilegiadas o crean, acceden, actualizan o eliminan cualquier registro. El impacto que sufra la empresa depende de los datos que se manejen. (OWASP Top 10, 2017, p. 11).

Comúnmente las fallas en este tipo de ataques conllevan a la divulgación, modificación o destrucción de la información no autorizada de los datos, o realizar una acción fuera de los parámetros permitidos que tiene el cliente. De acuerdo a OWASP Top 10 – 2017, las vulnerabilidades más comunes incluyen:

- Pasar por alto las comprobaciones de control de acceso.
- Obtener mayores privilegios de los permitidos, actuar como un usuario de la empresa sin haber iniciado sesión o tener los privilegios de un administrativo habiendo iniciado sesión siendo un cliente estándar.
- Reproducir y manipular tokens para el acceso, manipulación de las cookies o un campo para obtener mayores privilegios.
- La configuración incorrecta del intercambio de recursos de origen cruzado (CORS) permitiendo el acceso no autorizado a una API.
- Acceder a una API sin control de acceso mediante el uso de verbos POST, PUT y DELETE. (OWASP Top 10, 2017, p. 11).

Los controles para tratar de mitigar este tipo de ataques son solo efectivos si se realizan del lado del servidor, en donde el atacante no pueda modificar los datos, se tiene en cuenta según OWASP Top 10 -2017 lo siguiente:

- Implementar mecanismos de control de acceso una vez y reutilizarlos en toda la aplicación web.
- Los controles deben imponer las características que les quiera otorgar el dueño de la empresa, es decir, que los clientes no tengan libertad en crear, leer, actualizar o eliminar cualquier registro.
- Asegurarse que las copias de seguridad no se encuentren en las carpetas públicas y deshabilitar el listado de directorios de la aplicación web.
- Registrar los errores de control de acceso e informar a los administrativos cuando corresponda.
- Limitar la taza de acceso a la aplicación web para minimizar el daño de herramientas de ataques automatizados.
- Los tokens para el acceso deben ser invalidados luego de la finalización de la sesión. (OWASP Top 10, 2017, p. 11).

### *4.7.6. Configuración de seguridad incorrecta*

Los atacantes intentan a menudo explotar vulnerabilidades que se encuentran sin parchear, sin actualizar o acceder por cuentas por defecto, paginas no utilizadas, directorios desprotegidos, entre otras, con la finalidad de obtener acceso o conocimiento de la empresa. (OWASP Top 10, 2017, p. 12).

Una incorrecta configuración puede ocurrir en cualquier nivel de stack tecnológico, como puede ser la configuración de la aplicación web, máquinas virtuales, la base de datos, etc. Los analizadores de vulnerabilidades son de gran ayuda para detectar configuraciones erróneas, servicios innecesarios, configuraciones predeterminadas, etc. (OWASP Top 10, 2017, p. 12).

El impacto que sufra dependerá de la aplicación web a la que se le encuentre realizando el ataque, asi como de la concurrencia que se tendrá y de los datos que maneje la misma, ya que el atacante puede obtener acceso no autorizado a algunos datos o funciones del sistema. (OWASP Top 10, 2017, p. 12).

De acuerdo a OWASP Top 10 – 2017, el servicio web puede ser vulnerable a este tipo de ataques si:

- Permisos mal configurados en los servicios de la nube.
- Se encuentran instaladas características innecesarias como puertos, servicios, paginas, cuentas o permisos que puede utilizar el atacante.
- Las cuentas predeterminadas y las contraseñas siguen encontrándose activas y sin cambios.
- Las nuevas funciones de seguridad se encuentran desactivadas o no se encuentran configuradas de forma adecuada o segura.

- El servidor no envía cabeceras de seguridad a los clientes o se encuentran configurados con valores inseguros. (OWASP Top 10, 2017, p. 12).

Para prevenir este tipo de ataques, según OWASP Top 10 – 2017, en el momento de la implementación se debe incluir:

- Utilizar una plataforma minimalista sin funcionalidades innecesarias, componentes, documentación o ejemplos. Eliminando las funcionalidades no utilizadas.
- Seguir un proceso para revisar y actualizar las configuraciones apropiadas de acuerdo a las advertencias de seguridad y siga un proceso de gestión de parches.
- La empresa debe tener una arquitectura segmentada que proporcione una separación efectiva y segura entre componentes y a la vez controlar el acceso a terceros mediante la utilización de ACLs.
- Utilizar un proceso automatizado para verificar la efectividad de los ajustes y configuraciones en todos los ambientes. (OWASP Top 10, 2017, p. 12).

A continuación, se menciona algunos ejemplos en relación al presente tipo de ataque:

- La configuración del servidor permite retornar mensajes de error detallado a los clientes, esto expone información sensible o fallas subyacentes, tales como versiones de componentes que se saben que son vulnerables.
- El listado de directorios se encuentra activado en el servidor, un atacante descubre que puede listar estos archivos. El atacante puede realizar ingeniería inversa y encontrar un problema en el control de acceso de la aplicación web. (OWASP Top 10, 2017, p. 12).

### *4.7.8. Secuencia de comandos en sitios cruzados (XSS)*

XSS es la segunda vulnerabilidad más frecuente y se encuentra en general en dos tercios de todas las aplicaciones web, el impacto que genera a la empresa es moderado en el caso de XSS Reflejado y basado en DOM como puede ser la caída de los servicios web mediante la realización de ataques de denegación de servicio. El XSS almacenado permite ejecutar secuencias de comandos en el navegador de la víctima obteniendo credenciales, secuestrar sesiones o la instalación de softwares maliciosos en el equipo de la víctima. (OWASP Top 10, 2017, p. 13).

De acuerdo a OWASP Top 10 – 2017, existen tres formas para atacar a los usuarios mediante XSS las cuales son:

- XSS Reflejado: la aplicación o API utiliza datos sin validar suministrados por un usuario y codificados como parte del HTML. El usuario deberá interactuar con un enlace o una página controlada por el atacante, en el que se puede dar publicidad maliciosa o algo similar sobre la empresa.
- XSS Almacenado: la aplicación web almacena datos del usuario si validar, lo que posteriormente pueden ser utilizados por otro cliente o por un administrativo. Lo cual es considerado como un riesgo alto o crítico.
- XSS basado en DOM: aplicaciones de página única que incluye datos dinámicos controlables por un atacante. (OWASP Top 10, 2017, p. 13).

Los ataques XSS incluyen robo de la sesión, denegación de servicio, apropiación de la cuenta, inclusión de troyanos de autenticación, y otros tipos de ataques al lado del cliente. (OWASP Top 10, 2017, p. 13). Y para poder prevenir este tipo de ataques se toma en cuenta:

- Mantener los datos no confiables separados del contenido activo del navegador.
- Utilizar frameworks que, por diseño, automáticamente codifican el contenido para prevenir ataques XSS.
- Aplicar codificación, cuando se modifica el documento en el navegador del cliente, ayuda a prevenir XSS basado en DOM.
- Aplicar una defensa profunda según la política de seguridad, asumiendo que no se tiene otras vulnerabilidades que permitan colocar algún código malicioso. (OWASP Top 10, 2017, p. 13).

A continuación, se explican un escenario en el que se puede dar el ataque XSS. La aplicación utiliza datos no confiables en la construcción del código HTML sin validarlos o codificarlos. La finalidad es de la sesión del cliente sea enviada hacia el atacante, lo cual le permitirá secuestrar la sesión actual del cliente. (OWASP Top 10, 2017, p. 13).

#### *4.7.9. Deserialización insegura*

La realización de este tipo de ataque es muy difícil porque los exploits distribuidos muy raramente funcionan sin cambio o algún ajuste en su código fuente. Este tipo de ataque se lo incluye basado en una encuesta y no por datos cuantificables. (OWASP Top 10, 2017, p. 14).

Algunas herramientas pueden descubrir este tipo de vulnerabilidades, pero se necesita ayuda humana para validarlo. Se espera que las personas que desarrollan las diferentes herramientas vayan

aumentando y mejorando las mismas para poder identificarlos y abordarlos. (OWASP Top 10, 2017, p. 14).

Es una vulnerabilidad que se debe tener muy en cuenta ya que permite al atacante la ejecución remota del código, en donde, el impacto que se tenga a la aplicación web dependerá de la utilización que tenga la aplicación por los clientes o el tipo de datos que se guarden. (OWASP Top 10, 2017, p. 14).

Para poder saber si la aplicación web es vulnerable a este tipo de ataque, según OWASP Top 10 - 2017 se toma en cuenta:

- Ataques relacionados con la estructura de datos y objetos, aquí el atacante es capaz de modificar la lógica de la aplicación o de ejecutar códigos de forma remota alterando el comportamiento de la aplicación web.
- Ataques típicos de manipulación de datos, son ataques relacionados con el control de acceso, en el cual se modifica su contenido. (OWASP Top 10, 2017, p. 14).

Este tipo de ataques pueden ser utilizados en aplicaciones para:

- Comunicación remota a inter procesos.
- Protocolos de comunicaciones.
- Atrapar datos y persistencia.
- Bases de datos, servidores de cache y sistemas de archivos.

Según OWASP top 10 – 2017, para mitigar este tipo de ataques se debe tener en cuenta los siguientes puntos:

- No aceptar objetos serializados de fuentes no confiables.
- Implementación de verificación tales como firmas digitales, con el fin de identificar modificaciones no autorizadas.
- Aislar el código que se encarga de realizar la deserialización, con la finalidad de que ejecute en un entorno con la menor cantidad de privilegios posibles.
- Restringir y monitorear las conexiones que se realicen. (OWASP Top 10, 2017, p. 14).

#### *4.7.10. Componentes con vulnerabilidades conocidas*

Para vulnerabilidades ya conocidas es sencillo obtener diferentes exploits, lo que requiere un gran esfuerzo para el atacante es su desarrollo y/o personalización. Estos defectos están muy difundidos,

este tipo de vulnerabilidad es detectable con los analizadores de vulnerabilidades o mediante la inspección de cabeceras. (OWASP Top 10, 2017, p. 15).

Algunas de las mayores brechas o problemas que se han registrado han sido mediante la explotación de las vulnerabilidades conocidas en componentes comunes. Dependiendo la información que maneje la aplicación web, esta vulnerabilidad puede ser la principal de la lista. (OWASP Top 10, 2017, p. 15).

De acuerdo a OWASP TOP 10 – 2017, la aplicación web es potencialmente vulnerable si:

- No se conoce las versiones de todos los componentes que se utiliza.
- El software es vulnerable si no posee soporte o se encuentra desactualizado. Incluye el sistema operativo, aplicaciones web o el servidor.
- No analizar los componentes periódicamente ni se realiza informes acerca de los componentes utilizados.
- No se parchea o actualiza la plataforma subyacente, frameworks y dependencias, con un enfoque basado en riesgo. Esto sucede cuando las actualizaciones se realizan de forma mensual o trimestral. (OWASP Top 10, 2017, p. 15).

Para prevenir este tipo de vulnerabilidades se tiene en cuenta los siguientes puntos:

- Remover dependencias, funcionalidades, componentes, archivos y documentación innecesaria y no utilizada.
- Monitorear continuamente en búsqueda de vulnerabilidades en los componentes utilizados. Utilizar herramientas de análisis de vulnerabilidades.
- Obtener componentes únicamente de sitios autorizados u oficiales. Con el fin de disminuir versiones que pueden ser manipuladas maliciosamente.
- Supervisar bibliotecas y componentes que no poseen mantenimiento o no liberan parches de seguridad para sus versiones obsoletas o sin soportes. Si la realización del parcheo no es posible, intentar un parcheo virtual para monitorizar, detectar y/o protegerse contra la debilidad detectada. (OWASP Top 10, 2017, p. 15).

#### *4.7.11. Registro y monitoreo insuficientes*

El registro y monitoreo insuficiente de las empresas a sus aplicaciones web es comúnmente la base de casi todos los problemas de seguridad que se tienen. Los atacantes dependen gran parte de que no exista el monitoreo y respuesta oportuna para lograr sus objetivos. (OWASP Top 10, 2017, p. 16).

Un método para saber si se tiene un monitoreo suficiente, es el de analizar los registros que se tienen después de realizar las pruebas de penetración, las pruebas que realizaron los evaluadores deben registrarse lo suficiente para poder comprender los daños que pueden haber causado. (OWASP Top 10, 2017, p. 16).

Los ataques que tienen más éxito comienzan con la explotación de las vulnerabilidades que poseen las aplicaciones web, permitir que el análisis de vulnerabilidades continúe puede aumentar la probabilidad de que la prueba de penetración sea exitosa tanto para un evaluador como para un atacante. (OWASP Top 10, 2017, p. 16).

Para tener en cuenta, ya que se conoce que este tipo de vulnerabilidad puede ocurrir, según OWASP Top 10 – 2017, se toma en cuenta los siguientes puntos para ser identificados:

- Los inicios de sesión y transacciones de altos valores no son registrados.
- Advertencias y errores generan registros pocos claros, inadecuados o ninguno en absoluto.
- Registros en las aplicaciones web no son monitoreadas para detectar actividades sospechosas.
- Los registros son almacenados solo de forma local.
- Los umbrales de alerta y de escalamiento de respuesta no están implementados no son eficientes.
- La aplicación no logra detectar, escalar y/o alertar sobre ataques en tiempo real. (OWASP Top 10, 2017, p. 16).

De acuerdo a OWASP Top 10 – 2017, para poder prevenir este tipo de vulnerabilidad se debe tomar en cuenta el riesgo de los datos almacenados o procesados por la aplicación:

- Asegurar que todos los inicios de sesión, control de acceso y validación de entradas sean registrados, con la finalidad de identificar cuentas sospechosas. Mantener este análisis durante un tiempo adecuado para realizar un correcto análisis forense.
- Asegurar que las transacciones que se realicen mediante la aplicación web tenga controles de integridad para prevenir alteraciones o eliminaciones de datos.
- Cuando son transacciones de alto valor tener una base de datos que recopile con mayor cuidado.
- Establecer un monitoreo y alertas adecuadas, con la finalidad de que las actividades que sean sospechosas sean detectadas y sean resueltas dentro de periodos de tiempos aceptables. (OWASP Top 10, 2017, p. 16).

## CONCLUSIONES

- Las vulnerabilidades que se encontraron en el ambiente simulado de los servidores virtuales de licenciamiento libre que contienen los servicios web informativos de la ESPOCH son: ataques XSS, sobre carga del buffer, exploración de archivos y encabezado x-frame-Options no establecido.
- Las mejores practicas analizadas se tomo en cuenta de cada una de las metodologías lo siguiente: NIST 800 – 144 se toma en cuenta la información acerca de cloud computing, OWASP presenta las vulnerabilidades más dañinas en servicios web, ISSAF permite realizar la evaluación de seguridad en una organización con una secuencia de fases para el análisis y OSSTMM para conocer si la seguridad de los servidores se encuentra en los limites establecidos por la empresa.
- Se realizo una metodología hibrida analizando la NIST 800 – 144, OWASP, ISSAF y OSSTMM, tomando en cuenta de cada una de las metodologías anteiormente mencionadas los datos relacionados a los servidores virtuales, explicando las mayores vulnerabilidades que tienen los servicios web, las formas en que se pueden dar dichas vulnerabilidades y con su respectiva posible mitigación.
- Se utilizo la metodología hibrida propuesta utilizando las tres fases que son: planificación, desarrollo y resultados para la realización del presente trabajo de titulación en un ambiente simulado GNS3, en el cual se exploto la vulnerabilidad de la sobrecarga de buffer mediante los ataques de denegación de servicio SYN con slowloris y Metasploit, e implementando su correspondiente mitigación con mod_qos que fue existosa.

**RECOMENDACIONES**

- Se recomienda elegir un analizador de vulnerabilidades de acuerdo a las vulnerabilidades que se desea analizar como puede ser: servicios web, el trafico de una red, etc. Para con ello realizar las mejores correcciones a las vulnerabilidades que se presenten.
- Tomar en cuenta las diferentes metodologías existentes para cuando se realice alguna auditoria de una infraestructura de red, escoger la que mas se acople a los datos de la empresa y con ello mantenerla protegida de los diferentes ataques que se pueden presentar.
- Si se desea analizar una metodología hibrida tomar en cuenta la información que sea de mayor utilidad de las diferentes metodologías a analizar, como puede ser la información que desea proteger la empresa, ya que con ello los ataques y vulnerabilidades que se pueden tener pueden variar.
- Cuando se realiza un ambiente simulado tratar de obtener la mayor cantidad de la información para que la infraestructura que se replica trate de ser lo mas parecida a la real, guardando a la vez los datos sensibles que considere la empresa por motivos de políticas de seguridad.

**BIBLIOGRAFIA**

**ACUNETIX LTD.** *Acunetix Web Vulnerability Scanner* [En línea] Document versión 7. 2011. pp.8 [Consulta: 2019-09-28] Disponible en: https://www.acunetix.com/resources/wvs7manual.pdf

**ALACOT, Marco.** *Implantación de una plataforma de Clou Computing* [En línea] (Trabajo de titulación) (Ingeniería) Universitat Politécnica de Valencia, Valencia – Epaña. 2011. pp. 5-9 [Consulta: 2019-03-11]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/14103/memoria.pdf?sequence

**ALONSO, José; DÍAZ, Vicente; GUZMÁN, Antonio; LAGUNA, Pedro & BAILÓN, Alejandro.** *Seguridad en Base de datos* [En línea]. Universitat Oberta de Catalunya. Catalunya – España. 2012. pp. 14 [Consulta: 2019-09-28] Disponible en: https://www.exabyteinformatica.com/uoc/Informatica/Seguridad_en_bases_de_datos/Seguridad_en_bases_de_datos_(Intro).pdf

**ALVARADO, Aida & MONTESDEOCA, Richard.** *Análisis de vulnerabilidades del servidor E-learning de la ESPOCH para la implementación de mejores prácticas de seguridad-acceso* [En línea] (Trabajo de titulación) (Ingeniería) Escuela Superior Politécnica de Chimborazo, Riobamba – Ecuador. 2017. pp. 1-5 [Consulta: 2019-03-12]. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/6873/1/98T00152.pdf

**AMADO, John; AYALA, Carlos & SIERRA Armando**. *Analisis de vulnerabilidades en aplicaciones Web desarrolladas en PHP Versión 5.6.24 con base de datos MYSQL Versión 5.0.11 a partir de ataques SQL Inyección* [En línea] (Trabajo de titulación) (Ingeniería) Universidad de Cooperativa de Colombia. Bucaramanga - Colombia. 2017. pp. 1-5. [Consulta: 2019-03-11]. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/1651/1/Análisis%20de%20vulnerabilidades%20en%20aplicaciones%20Web%20desarrolladas%20en%20PHP%20Versión%205.6.24%20con%2

0base%20de%20datos%20MYSQL%20Versión%205.0.11%20a%20partir%20de%20ataques%20SQL%20Inyección%20-%20copia.pdf

**BADILLO, David & CHAFLA, Gustavo**. *Estudio Comparativo de las distribuciones Linux orientado a la seguridad de las redes de comunicación* [En línea] (Trabajo de titulación) (Maestría) Pontifica Universidad Católica del Ecuador. Quito - Ecuador. 2015. pp. 1-5 [Consulta: 2019-03-11]. Disponible en: http://repositorio.puce.edu.ec/bitstream/handle/22000/10002/TESISV25-26-11-2015.pdf?sequence=1&isAllowed=y

**BARRIO, Santiago.** *Cluster Alta Disponibilidad sobre Plataforma GNU/LINUX* [En línea] (Trabajo de titulación) (Ingeniería). Universitat Oberta de Catalunya. Catalunya – España. 2011. pp. 1-2 [Consulta: 2019-03-15] Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/29841/6/sbarrioTFC0114memoria.pdf

**BERNARD, Jansen; RAMASAMY, HariGovind & SCHUNTER, Matthias.** *Flexible Integrity Protection and Verification Architecture for Virtual Machine Monitors* [En línea]. IBM Zurich Research Laboratory, Ruschlikon – Switzerland. 2011. pp. 1-5 [Consulta: 2019-03-15] Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.566.9383&rep=rep1&type=pdf

**CHRISTEY, Steve & MARTIN, Rober.** *Vulnerability Type Distributions in CVE* [En línea]. 2007. Mitre Report. pp. 1-38 [Consulta: 2019-03-17] Disponible en: http://cwe.mitre.org/documents/vuln-trends/vuln-trends.pdf

**CRUZ, Yolanda & MARTÍNEZ, Carlos.** *Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final* [En línea]. 2017. Revista científica Dominio de las Ciencias. pp. 506 [Consulta: 2019-03-18] Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6128529

**DESHMUKH, Rashmi & DEVADKAR, Kailas.** *Understanding DDoS Attack & its Effect in Cloud Environment* [En línea]. 2015. Procedia Computer Science 49. pp. 5-6 [Consulta: 2019-03-17] Disponible en: https://www.sciencedirect.com/science/article/pii/S1877050915007541

**DIARMUND, O'Brian.** *Virtualization with the Kernel-based Virtual Machine ( KVM )* [En línea] Communications/computing/security C2S. 2017, pp. 8-10 [Consulta: 2019-03-20] Disponible en: http://www.obriain.com/training/virtualisation/odt/Virtualisation_with_KVM_v2.2.pdf

**DOÑA, Jesús; GARCÍA, Juan; LÓPEZ, Jesús; PASCUAL, Francisco & PASCUAL, Rubén.** *Virtualizacion de Servidores. Una solucion de Futuro, Área de Tecnología y Sistemas de Información*, [En línea] (Paper) Campus Universitario de Teatinos, Malaga - España. 2010. pp. 1-5. [Consulta: 2019-03-11]. Disponible en: http://www.redtauros.com/Clases/Gestion_SO/Sistemas_paravirtuales.pdf

**GALMÉS, Andrés.** *Sobre la seguridad del almacenamiento en la nube* [En línea] (Trabajo de titulación) (Maestría) Universitat Oberta de Catalunya, Catalunya – España. 2016. pp. 9-10 [Consulta: 2019-03-12]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/45887/1/Agalmesh_TFM_0116.pdf

**GKORTZIS, Antonios; RIZOU, Stamatia & SPINELLIS, Diomidis.** *An empirical analysis of vulnerabilities in virtualization technologies* [En línea]. Department of Management Science and Technology. European Projects Department. Athens – Greece. 2016. pp. 1-10 [Consulta: 2019-03-15] Disponible en: https://fsdet.dmst.aueb.gr//wp-content/uploads/2017/05/14_FSDET_paper_33.pdf

**GÓMEZ, Juan.** *Kernel Based Virtual Machine ( KVM ) - Base de Conocimimento.* [En línea]. 2012. pp. 1-3 [Consulta: 2019-03-20] Disponible en: https://es.scribd.com/document/83132428/Kernel-Based-Virtual-Machine-KVM-Base-de-Conocimiento

**GUTIÉRREZ, Alfredo.** *Virtualización de servidores de la infraestructura informática de la Universidad de Quinta Roo, Unidad Chetumal* [En línea] (Trabajo de titulación) (Ingeniería) Universidad de Quinta Roo, Quinta Roo – México. 2014. pp. 7-11 [Consulta: 2019-03-14]. Disponible en: http://risisbi.uqroo.mx/bitstream/handle/20.500.12249/495/QA76.9.C55.G98.2014-381.pdf?sequence=1&isAllowed=y

**HURTARES J. & CAMINOS V.** *Virtualización, diseño e implementación de central de voz sobre ip* [En línea]. Escuela Superior Politécnica del Litora. Guayaquil – Ecuador. 2012. pp. 4-6 [Consulta: 2019-03-19] Disponible en: https://www.dspace.espol.edu.ec/bitstream/123456789/31911/1/VIRTUALIZACION%2C%20DISEÑO%20E%20IMPLEMENTACIÓN%20DE%20CENTRAL%20DE%20VOZ%20SOBRE%20IP.pdf

**ISECOM.** *The Open Source Security Testing Methodology Manual.* Institue for Security and Open Methodology (ISECOM). 2011

**JIMÉNEZ, David.** Privacy and Confidentiality issues in Cloud Computing architectures [En línea] (Trabajo de titulación) (Maestría). Universitat Politécnica de Catalunya. Catalunya – España. 2013. pp. 61-63 [Consulta: 2019-03-16] Disponible en: https://upcommons.upc.edu/bitstream/handle/2099.1/20816/thesis-david.jimenez-martinez-1.pdf

**JONES, Kathryn & GONZÁLEZ, Esteban.** *Secretos del VM: Virtualización y Drivers*, [En línea] (Paper) Universidad de Costa Rica, San José - Costa Rica. 2008. pp. 3-12. [Consulta: 2019-03-11]. Disponible en: http://www.di-mare.com/adolfo/cursos/2008-2/pp-VM.pdf

**LANDI, Veronica.** *Estudio, Análisis y Diseño para la virtualización de la infraestructura de servidores utilizando una red de almacenamiento en la empresa Impordemin CIA. LTDA* [En línea] (Trabajo de titulación) (Ingeniería) Universidad Politécnica Salesiana. Quito – Ecuador. 2013. pp. 1-5. [Consulta: 2019-03-11]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/4166/6/UPS%20-%20ST000958.pdf

**LEVINA, Olga; OETTING, Jan & CHOU, Yuyu.** *Enforcing Confidentiality in a SaaS Cloud Enviroment* [En línea]. 2011. 19th Telecommunications fórum TELFOR 2011. pp. 1-4 [Consulta: 2019-03-16] Disponible en: https://ieeexplore.ieee.org/document/6143500

**LITCHFIELD, Alan & SHAHZAD, Abid.** *A Systematic Review of Vulnerabilities in Hypervisors and Their Detection* [En línea]. 2017. Twenty-third Americas Conference on Information Systems. Boston – EEUU. pp. 2-6 [Consulta: 2019-03-17] Disponible en: https://pdfs.semanticscholar.org/25f9/79225153aaaec873ef238bec363cd600292e.pdf

**LÓPEZ, Dayana & RAMÍREZ, Pavel.** *Pruebas de seguridad utilizando herramientas para la detección de vulnerabilidades* [En línea] La Habana Cuba, del 19 al 23 de marzo. 2018. pp. 3-5 [Consulta: 2019-09-28] Disponible en: http://www.informaticahabana.cu/sites/default/files/ponencias2018/CAL28.pdf

**LÓPEZ, Roberto.** *Propuesta de implementación de una metodología de auditoría de seguridad informática* [En línea] (Trabajo de titulación) (Ingeniería). Universidad Autónoma de Madrid. Madrid – España. 2015. pp. 17-24 [Consulta: 2019-03-18] Disponible en: https://repositorio.uam.es/handle/10486/668900

**MÁRQUEZ, Alex & SOLANO, Luis.** *Virtualización de servidores* [En línea] (Trabajo de titulación) (Ingeniería) Universitat Politécnica de Catalunya, Barcelona – España. 2011. pp. 7-8 [Consulta: 2019-03-13] Disponible en: https://core.ac.uk/download/pdf/41794509.pdf

**MÁRQUEZ, Berta & ZULAICA, José.** *Implementación de un reconocedor de voz gratuito a el sistema de ayuda a invidentes Dos-Vox en español* [En línea] (Trabajo de titulación) (Licenciatura) Universidad de las Américas Puebla, Puebla – México. 2004. pp. 1-4 [Consulta: 2019-03-13]. Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/marquez_a_bm/

**MONAR, Joffre.** *Propuesta de un método utilizando técnicas de programación seguras para el desarrollo de aplicaciones web en entornos PHP para mitigar riesgos potenciales de seguridad* [En línea] (Trabajo de titulación) (Maestría) Escuela Superior Politécnica de Chimborazo. Riobamba – Ecuador. 2017. pp. 42-43 [Consulta: 2019-09-28] Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/6749/1/20T00857.pdf

**NATIONAL INSTITUE OF STANDARDS AND TECHNOLOGY.** *Guidelines on Security and Privacy in Public Cloud Computing*, U.S. Department of Commerce, Special Publication 800-144.

**OISSG.** *Information Systems Security Assesment Framework (ISSAF).* Open Information Systems Security Group (OISSG). 2006.

**ORACLE VM VIRTUAL BOX.** *User Manual* [En línea]. 2004-2017. pp. 1-4 [Consulta: 2019-09-28] Disponible en: https://download.virtualbox.org/virtualbox/5.1.22/UserManual.pdf

**ORTEGA, Samuel.** *Diseño de un sistema de seguridad para un servidor Web Apache* [En línea] (Trabajo de titulación) (Ingeniería) Universidad Politécnica de Madrid. Madrid – España. 2018. pp. 85-86. [Consulta: 2019-09-01] Disponible en: http://oa.upm.es/53223/1/TFG_SAMUEL_ORTEGA_SANCHO.pdf

**OWASP.** *Open Web Application Security Project.* 2017 [En línea]. [Consulta: 2019-09-28]. Disponible en: https://www.owasp.org/images/2/2d/OWASP_Top_10_-_2010_FINAL_(spanish).pdf

**OWASP TOP 10 – 2017.** *Los diez riesgos más críticos en aplicaciones web* [En línea]. Creative Commons Attribution-ShareAlike 4.0 International License. 2017. pp. 26-28 [Consulta: 2019-09-28] Disponible en: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

**PRATS, Jordi; VEGA, Ricard & CAMBRAS, Joan.** *Virtualización y alta disponibilidad para entornos de hospedaje y desarrollo de portales web* [En línea]. Boletín de RedIRIS, 2008, n° 82-83 [Consulta: 2019-03-15] Disponible en: https://www.rediris.es/difusion/publicaciones/boletin/82-83/ponencia1.4C.pdf

**TAKEMURA, Chris & CRAWFORD, Luke.** *The book of XEN, A practica guide for the system administrator* [En línea]. No Starch Press; Edición: 1. 2009. pp. 5-6 [Cosulta: 2019-03-18] Disponible en: https://www.amazon.es/Book-Xen-Practical-System-Administrator/dp/1593271867

**TARAZONA, Cesar.** *Amenazas informáticas y seguridad de la información* [En línea]. Universidad Externado de Colombia. Bogotá – Colombia. 2007. pp. 137 [Consulta: 2019-03-15] Disponible en: https://revistas.uexternado.edu.co/index.php/derpen/article/view/965

**TIERRA, María & BONILLA, Jéssica.** *Análisis comparativo del performance de hipervisores bare-metal aplicado a la implementación de servicios corporativos TCP/IP más usados en las instituciones públicas de Riobamba* [En línea] (Trabajo de titulación) (Ingeniería) Escuela Superior Politécnica de Chimborazo, Riobamba – Ecuador. 2014. pp. 40-42. [Consulta: 2019-03-15] Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/3572/1/18T00560.pdf

**TOAPANTA, Defaz; YANCHAPAXI, Ximena & ORESTILA Ruth.** *Análisis de la aplicación metodológica para el estudio de riesgos y vulnerabilidades en la Universidad de Pinar del Río: Propuesta de Perfeccionamiento* [En línea] (Trabajo de titulación) (Ingeniería). Universidad Técnica de Cotopaxi. Latacunga – Ecuador. 2006. pp. 8-10 [Consulta: 2019-03-15] Disponible en: http://repositorio.utc.edu.ec/handle/27000/536

**VILLAR, Eugenio; LÓPEZ, Julio & MONTOYA, Francisco**. *Virtualización de servidores de telefonía IP en GNU/Linux* [En línea] (Trabajo de titulación) (Ingeniería) Universidad de Almería, Almeria – España. 2010. pp. 16-27 [Consulta: 2019-03-13]. Disponible en: http://www.adminso.es/images/d/dc/PFC_eugenio.pdf

**XIAO, Zhifeng & XIAO, Yang.** *Security and Privacy in Cloud Computing* [En línea]. 2013. IEEE Communications surveys & tutorials. Vol. 15. N° 2. pp. 843-845 [Consulta: 2019-03-16] Disponible en: https://s3.amazonaws.com/academia.edu.documents/31786964/1.pdf?response-content-disposition=inline%3B%20filename%3DSecurity_and_Privacy_in_Cloud_Computing.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20191016%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191016T210530Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=ac8331b157438a1459c902298c6de4d18da24494e5e271285c6207495bbc8f0e

**ZHOU, Minqi; ZHANG, Rong; XIE Wei; QIAN, Qeining & ZHOU, Aoying.** *Security and Privacy in Cloud Computing: A Survey* [En línea]. 2010. Sixth International Conference on Semantics, Knowledge and Grids. 62 [Consulta: 2019-03-16] Disopnible en: https://www.researchgate.net/profile/Weining_Qian/publication/224204127_Security_and_Privacy_in_Cloud_Computing_A_Survey/links/55b6f75e08ae092e9656f9a5/Security-and-Privacy-in-Cloud-Computing-A-Survey.pdf

**ANEXOS**

**ANEXO A:** OFICIO PARA ACCEDER A LA INFORMACIÓN DEL DTIC.

Riobamba, 10 de enero de 2019

DTIC - ESPOCH
RECIBIDO
10 ENE 2019
POR: Paulo B

Ingeniero
Juan Carlos Díaz
**DIRECTOR DEL ÁREA DEL DTIC**

De mi consideración.-

Con un cordial y atento saludo, solicito de la manera más atenta a usted se facilite un permiso para acceder a la infraestructura de la red de la ESPOCH, con la finalidad de realizar una investigación sobre el anteproyecto de tesis: "Análisis de vulnerabilidades de servidores virtuales para la ESPOCH", presentado por el señor Ángel Salvador Arias Paredes con cedula de identidad: 0604061838, estudiante de la Escuela de Ingeniería en Electrónica Telecomunicaciones y Redes de la FIE. Es de recalcar que la intención del permiso es para tener una concepción de la infraestructura para crear una simulación para el desarrollo de la tesis sin intervenir en la infraestructura actual ni divulgar configuración real alguna, que vulnere la política de seguridad institucional.

Sin más por el momento, agradezco su atención al presente oficio y quedo a la espera de su amable respuesta. Reciba un cordial saludo.

Atentamente,
"Saber para Ser"

Ing. Marco Vinicio Ramos Valencia Msc.
Docente de la Facultad de Informática y Electrónica

**ANEXO B:** OFICIO PARA OBTENER LA INFORMACIÓN DE ESTUDIANTES MATRICULADOS.

Riobamba, 06 de mayo de 2019

Ingeniera

Landy Ruiz Mancero

SECREATARIA ACADÉMICA DE GRADO ESPOCH

Presente

De mi consideración:

Yo, Ángel Salvador Arias Paredes con C.I. No 060406183-8, estudiante egresado de la Facultad de Informática y Electrónica solicito muy comedidamente me facilite la información del número total de estudiantes que se encuentran matriculados en la Escuela Superior Politécnica de Chimborazo (ESPOCH) y en la Facultad de Informática y Electrónica (FIE) en el periodo Marzo 2019 – Julio 2019, con la finalidad de la realización de una tesis titulada "Análisis de vulnerabilidades de servidores virtuales, caso práctico servicios web informativos de la ESPOCH".

Por su gentil atención, anticipo mi agradecimiento.

Cordialmente,

Ángel Salvador Arias Paredes

**ANEXO C:** INFORMACIÓN DEL NÚMERO DE ESTUDIANTES MATRICULADOS EN LA ESPOCH.

**ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO**

**SECRETARIA ACADEMICA GENERAL**

**Reporte del Número de Matrículas por Período Académico**

| Período Académico: 6 MARZO - 26 JULIO 2019 | |
|---|---|
| **Facultad: ADMINISTRACIÓN DE EMPRESAS** | |
| **Unidad Académica** | **Matrículas** |
| INGENIERIA EN CONTABILIDAD Y AUDITORIA | 266 |
| INGENIERIA DE EMPRESAS | 221 |
| ADMINISTRACIÓN DE EMPRESAS | 68 |
| INGENIERÍA EN MARKETING | 146 |
| MARKETING | 87 |
| CONTABILIDAD Y AUDITORIA | 28 |
| ADMINISTRACIÓN DE EMPRESAS . | 343 |
| INGENIERIA COMERCIO EXTERIOR | 1 |
| INGENIERIA COMERCIAL | 3 |
| INGENIERIA FINANCIERA | 252 |
| FINANZAS | 57 |
| INGENIERIA EN GESTION DE TRANSPORTE | 247 |
| GESTION DEL TRANSPORTE | 24 |
| CONTABILIDAD Y AUDITORIA . | 389 |
| CONTABILIDAD Y AUDITORIA (EXTENSIÓN MORONA SANTIAGO) | 165 |
| FINANZAS . | 382 |
| GESTION DEL TRANSPORTE . | 280 |
| MERCADOTECNIA . | 248 |
| **Total Facultad:** | **3207** |

# ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

## SECRETARIA ACADEMICA GENERAL

## Reporte del Número de Matrículas por Período Académico

**Período Académico: 6 MARZO - 26 JULIO 2019**

**Facultad: CIENCIAS**

| Unidad Académica | Matrículas |
|---|---|
| BIOQUIMICA Y FARMACIA . | 382 |
| BIOFISICA | 115 |
| BIOQUIMICA Y FARMACIA | 273 |
| ESTADISTICA | 116 |
| FISICA | 105 |
| INGENIERIA AMBIENTAL | 221 |
| INGENIERIA AMBIENTAL (EXTENSION NORTE AMAZONICA) | 144 |
| INGENIERÍA AMBIENTAL (EXTENSIÓN MORONA SANTIAGO) | 122 |
| BIOTECNOLOGIA AMBIENTAL | 403 |
| INGENIERIA EN ESTADISTICA INFORMATICA | 106 |
| INGENIERIA QUIMICA | 277 |
| INGENIERIA QUIMICA . | 362 |
| MATEMATICA | 96 |
| QUIMICA | 79 |
| QUIMICA . | 151 |
| **Total Facultad:** | **2952** |

**Facultad: CIENCIAS PECUARIAS**

| Unidad Académica | Matrículas |
|---|---|
| AGROINDUSTRIA | 297 |
| INGENIERIA EN INDUSTRIAS PECUARIAS | 222 |
| INGENIERIA ZOOTECNICA | 248 |
| ZOOTECNIA (EXTENSIÓN NORTE AMAZÓNICA) | 69 |
| ZOOTECNIA (EXTENSIÓN MORONA SANTIAGO) | 105 |
| ZOOTECNIA . | 243 |
| **Total Facultad:** | **1184** |

# ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

## SECRETARIA ACADEMICA GENERAL

## Reporte del Número de Matrículas por Período Académico

| Período Académico: 6 MARZO - 26 JULIO 2019 | |
|---|---|
| **Facultad: INFORMÁTICA Y ELECTRÓNICA** | |
| **Unidad Académica** | **Matrículas** |
| DISENO GRAFICO . | 179 |
| INGENIERIA EN ELECTRONICA CONTROL Y REDES INDUSTRIALES | 220 |
| INGENIERIA EN ELECTRONICA, TELECOMUNICACIONES Y REDES | 188 |
| INGENIERIA EN SISTEMAS | 146 |
| INGENIERIA EN SISTEMAS (EXTENSIÓN MORONA SANTIAGO) | 6 |
| ELECTRONICA Y AUTOMATIZACION . | 306 |
| INGENIERÍA EN DISENO GRAFICO | 123 |
| DISENO GRAFICO | 14 |
| SOFTWARE. | 284 |
| TELECOMUNICACIONES . | 297 |
| **Total Facultad:** | **1763** |
| **Facultad: MECÁNICA** | |
| **Unidad Académica** | **Matrículas** |
| INGENIERIA AUTOMOTRIZ | 261 |
| INGENIERIA INDUSTRIAL | 298 |
| INGENIERIA MECANICA | 236 |
| INGENIERIA DE MANTENIMIENTO | 251 |
| INGENIERIA AUTOMOTRIZ . | 401 |
| INGENIERIA INDUSTRIAL . | 366 |
| INGENIERIA MECANICA . | 341 |
| MANTENIMIENTO INDUSTRIAL . | 247 |
| **Total Facultad:** | **2401** |

# ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

## SECRETARIA ACADEMICA GENERAL

## Reporte del Número de Matrículas por Período Académico

| Período Académico: 6 MARZO - 26 JULIO 2019 | |
|---|---|
| **Facultad: RECURSOS NATURALES** | |
| **Unidad Académica** | **Matrículas** |
| AGRONOMIA . | 214 |
| INGENIERIA AGRONOMICA | 148 |
| INGENIERIA EN ECOTURISMO | 129 |
| INGENIERIA FORESTAL | 177 |
| ECOTURISMO | 69 |
| INGENIERIA FORESTAL . | 172 |
| AGRONOMIA (EXTENSIÓN NORTE AMAZÓNICA) | 91 |
| INGENIERÍA GEOLOGÍA Y MINAS (EXTENSION MORONA SANTIAGO) | 2 |
| MINAS (EXTENSION MORONA SANTIAGO) | 101 |
| RECURSOS NATURALES RENOVABLES | 141 |
| TURISMO (EXTENSION NORTE AMAZONICA) | 117 |
| TURISMO. | 117 |
| **Total Facultad:** | **1478** |
| **Facultad: SALUD PÚBLICA** | |
| **Unidad Académica** | **Matrículas** |
| GASTRONOMIA | 132 |
| MEDICINA | 912 |
| NUTRICION Y DIETETICA | 331 |
| GASTRONOMIA . | 181 |
| MEDICINA . | 668 |
| PROMOCION Y CUIDADOS DE LA SALUD | 239 |
| NUTRICION Y DIETETICA . | 342 |
| **Total Facultad:** | **2805** |

# ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

## SECRETARIA ACADEMICA GENERAL

## Reporte del Número de Matrículas por Período Académico

| Período Académico: 6 MARZO - 26 JULIO 2019 | |
|---|---|
| Facultad: UNIDAD DE NIVELACION Y ADMISION | |
| Unidad Académica | Matrículas |
| ARTES | 63 |
| AGRICULTURA RECURSOS NATURALES | 191 |
| AGRICULTURA (EXTENSIÓN MORONA SANTIAGO) | 26 |
| AGRICULTURA (EXTENSIÓN NORTE AMAZÓNICA) | 66 |
| AGRICULTURA PECUARIAS | 153 |
| COMERCIAL | 306 |
| COMERCIAL (EXTENSIÓN MORONA SANTIAGO) | 37 |
| CIENCIAS E INGENIERIA INFORMATICA Y ELECTRONICA | 213 |
| CIENCIAS E INGENIERIA CIENCIAS | 289 |
| CIENCIAS E INGENIERIA (EXTENSIÓN MORONA SANTIAGO) | 79 |
| CIENCIAS E INGENIERIA (EXTENSIÓN NORTE AMAZÓNICA) | 68 |
| CIENCIAS E INGENIERIA MECANICA | 774 |
| CIENCIAS E INGENIERIA INFORMATICA SOTFWARE FISICA MATEMATICAS | 260 |
| SERVICIOS GASTRONOMIA | 64 |
| SALUD MEDICINA Y NUTRICION | 177 |
| SERVICIOS (EXTENSIÓN NORTE AMAZÓNICA) | 29 |
| SERVICIOS TURISMO | 59 |
| SERVICIOS TRANSPORTE | 88 |
| Total Facultad: | 2942 |
| Total Período Académico (6 MARZO - 26 JULIO 2019): | 18.732,00 |

# ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

## SECRETARIA ACADEMICA GENERAL

## Reporte del Número de Matrículas por Período Académico

### Número Total de Estudiantes por Período Académico


**Promedio de Estudiantes: 18732.00**

**ANEXO D:** ENCUESTA REALIZADA PARA LA RECOLECCIÓN DE INFORMACIÓN DE LOS SERVICIOS WEB INFORMATIVOS DE LA ESPOCH.

1. ¿En qué facultad estudia en la Escuela Superior Politécnica de Chimborazo? _____

2. De los siguientes sistemas operativos, marque con una X el sistema operativo desde el menos utilizado hasta el más utilizado por usted.

| | Nunca | Casi nunca | A veces | Casi siempre | siempre |
|---|---|---|---|---|---|
| Linux | | | | | |
| Windows 7 | | | | | |
| Windows 8 | | | | | |
| Windows 10 | | | | | |
| Android | | | | | |

3. De los siguientes dispositivos, señale con una X desde el dispositivo que menos utiliza hasta el que más utiliza para ingresar a los servicios web informativos de la ESPOCH.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| Laptop | | | | | |
| Desktop | | | | | |
| Celular | | | | | |
| Tablet | | | | | |

4. De los siguientes servicios web informativos de la ESPOCH, señale con una X cuales son a los que ingresa con mayor frecuencia. Seleccionar 5 opciones desde el servicio web informativo menos utilizado hasta el más utilizado.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| DTIC | | | | | |
| Sistema web institucional | | | | | |
| Sistema e-Salud ESPOCH (Medicina) | | | | | |
| Bienestar estudiantil | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Talento humano | | | | | |
| Club de robótica ESPOCH | | | | | |
| Unidad de admisión y nivelación | | | | | |
| Página de la faculta de administración de empresas (FADE) | | | | | |

5. ¿Cómo definiría los servicios web informativos que ofrece la ESPOCH? Señale con una X.

| Muy malo | Malo | Regular | Bueno | Excelente |
|---|---|---|---|---|
| | | | | |

6. ¿Tiene conocimiento alguno sobre la seguridad de la información cuando accede a los servicios web informativos de la ESPOCH? Señale con una X.

| Muy bajo | Bajo | Medio | Alto | Muy alto |
|---|---|---|---|---|
| | | | | |

7. ¿De qué forma protege su dispositivo cuando navega para acceder a los servicios web informativos de la ESPOCH? Señale con una X desde la manera menos utilizada hasta la más utilizada que realiza para proteger su dispositivo.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| Antivirus. | | | | | |
| Firewall. | | | | | |
| Verificar los sitios a los que accede. | | | | | |
| Verificar las redes a las que se conecta. | | | | | |
| Navegar sin ningún parámetro. | | | | | |

8. Cuando accede a los servicios web informativos de la ESPOCH, ¿Usted toma las medidas adecuadas de seguridad para tener protegida su información? Señale con una X.

| Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|
| | | | | |

9. ¿Considera satisfactorio los servicios web informativos, es decir, de fácil utilización para el usuario los servicios web informativos de la ESPOCH? Señale con una X.

| Insatisfactorio | Poco satisfactorio | Medianamente satisfactorio | Satisfactorio | Muy satisfactorio |
|---|---|---|---|---|
| | | | | |

10. ¿Con que frecuencia accede a los servicios web de la ESPOCH?

| Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|
| | | | | |

11. ¿Qué tipo de conexión usa con mayor frecuencia para acceder a los servicios web informativos de la ESPOCH? Señale con una X desde el tipo de conexión menos utilizado hasta el más utilizado.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| Wii – Fi (Internet casa) | | | | | |
| Redes 2G | | | | | |
| Redes 3G | | | | | |
| Redes 4G | | | | | |
| Internet publico | | | | | |

**ANEXO E:** ENCUESTAS RESPONDIDAS POR ESTUDIANTES DE LA ESPOCH.

1. ¿En qué facultad estudia en la Escuela Superior Politécnica de Chimborazo?
   Recursos Naturales

2. De los siguientes sistemas operativos, marque con una X el sistema operativo desde el menos utilizado hasta el más utilizado por usted.

| | Nunca | Casi nunca | A veces | Casi siempre | siempre |
|---|---|---|---|---|---|
| Linux | | | X | | |
| Windows 7 | | | X | | |
| Windows 8 | | | X | | |
| Windows 10 | | | | | X |
| Android | | | X | | |

3. De los siguientes dispositivos, señale con una X desde el dispositivo que menos utiliza hasta el que más utiliza para ingresar a los servicios web informativos de la ESPOCH.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| Laptop | | | | | X |
| Desktop | | X | | | |
| Celular | | X | | | X |
| Tablet | | | | | |

4. De los siguientes servicios web informativos de la ESPOCH, señale con una X cuales son a los que ingresa con mayor frecuencia. Seleccionar 5 opciones desde el servicio web informativo menos utilizado hasta el más utilizado.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| DTIC | | | | | |
| Sistema web institucional | X | | | | |
| Sistema e-Salud ESPOCH (Medicina) | X | | | | |
| Bienestar estudiantil | X | | | | |
| Talento humano | X | | | | |
| Club de robótica ESPOCH | | | | | |
| Unidad de admisión y nivelación | X | | | | |
| Página de la faculta de administración de empresas (FADE) | | | | | X |

5. ¿Cómo definiría los servicios web informativos que ofrece la ESPOCH? Señale con una X.

| Muy malo | Malo | Regular | Bueno | Excelente |
|---|---|---|---|---|
| | | X | | |

6. ¿Tiene conocimiento alguno sobre la seguridad de la información cuando accede a los servicios web informativos de la ESPOCH? Señale con una X.

| Muy bajo | Bajo | Medio | Alto | Muy alto |
|---|---|---|---|---|
| | | | X | |

7. ¿De qué forma protege su dispositivo cuando navega para acceder a los servicios web informativos de la ESPOCH? Señale con una X desde la manera menos utilizada hasta la más utilizada que realiza para proteger su dispositivo.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| Antivirus. | | | X | | |
| Firewall. | | | | | |
| Verificar los sitios a los que accede. | | | X | | |
| Verificar las redes a las que se conecta. | | | | X | |
| Navegar sin ningún parámetro. | | | | | X |

8. Cuando accede a los servicios web informativos de la ESPOCH, ¿Usted toma las medidas adecuadas de seguridad para tener protegida su información? Señale con una X.

| Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|
| | | X | | |

9. ¿Considera satisfactorio los servicios web informativos, es decir, de fácil utilización para el usuario los servicios web informativos de la ESPOCH? Señale con una X.

| Insatisfactorio | Poco satisfactorio | Medianamente satisfactorio | Satisfactorio | Muy satisfactorio |
|---|---|---|---|---|
| | X | | | |

10. ¿Con que frecuencia accede a los servicios web de la ESPOCH?

| Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|
| | | | | X |

11. ¿Qué tipo de conexión usa con mayor frecuencia para acceder a los servicios web informativos de la ESPOCH? Señale con una X desde el tipo de conexión menos utilizado hasta el más utilizado.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| Wii – Fi (Internet casa) | | X | | | |
| Redes 2G | | | X | | |
| Redes 3G | | X | | | |
| Redes 4G | | | X | | |
| Internet publico | | X | | | |

1. ¿En qué facultad estudia en la Escuela Superior Politécnica de Chimborazo?
Ing Química

2. De los siguientes sistemas operativos, marque con una X el sistema operativo desde el menos utilizado hasta el más utilizado por usted.

| | Nunca | Casi nunca | A veces | Casi siempre | siempre |
|---|---|---|---|---|---|
| Linux | X | | | | |
| Windows 7 | | | X | | |
| Windows 8 | | | X | | |
| Windows 10 | | | X | | |
| Android | | | X | | |

3. De los siguientes dispositivos, señale con una X desde el dispositivo que menos utiliza hasta el que más utiliza para ingresar a los servicios web informativos de la ESPOCH.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| Laptop | | | | | X |
| Desktop | X | | | | |
| Celular | | | | | X |
| Tablet | | X | | | |

4. De los siguientes servicios web informativos de la ESPOCH, señale con una X cuales son a los que ingresa con mayor frecuencia. Seleccionar 5 opciones desde el servicio web informativo menos utilizado hasta el más utilizado.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| DTIC | | X | | | |
| Sistema web institucional | | | | | X |
| Sistema e-Salud ESPOCH (Medicina) | | X | | | |
| Bienestar estudiantil | | | X | | |
| Talento humano | | X | | | |
| Club de robótica ESPOCH | X | | | | |
| Unidad de admisión y nivelación | | | | | X |
| Página de la faculta de administración de empresas (FADE) | X | | | | |

5. ¿Cómo definiría los servicios web informativos que ofrece la ESPOCH? Señale con una X.

| Muy malo | Malo | Regular | Bueno | Excelente |
|---|---|---|---|---|
| | | | X | |

6. ¿Tiene conocimiento alguno sobre la seguridad de la información cuando accede a los servicios web informativos de la ESPOCH? Señale con una X.

| Muy bajo | Bajo | Medio | Alto | Muy alto |
|---|---|---|---|---|
| | | X | | |

7. ¿De qué forma protege su dispositivo cuando navega para acceder a los servicios web informativos de la ESPOCH? Señale con una X desde la manera menos utilizada hasta la más utilizada que realiza para proteger su dispositivo.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| Antivirus. | | X | | | |
| Firewall. | | X | | | |
| Verificar los sitios a los que accede. | | | X | | |
| Verificar las redes a las que se conecta. | | | X | | |
| Navegar sin ningún parámetro. | | | | X | |

8. Cuando accede a los servicios web informativos de la ESPOCH, ¿Usted toma las medidas adecuadas de seguridad para tener protegida su información? Señale con una X.

| Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|
| | X | | | |

9. ¿Considera satisfactorio los servicios web informativos, es decir, de fácil utilización para el usuario los servicios web informativos de la ESPOCH? Señale con una X.

| Insatisfactorio | Poco satisfactorio | Medianamente satisfactorio | Satisfactorio | Muy satisfactorio |
|---|---|---|---|---|
| | X | | | |

10. ¿Con que frecuencia accede a los servicios web de la ESPOCH?

| Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|
| | | | X | |

11. ¿Qué tipo de conexión usa con mayor frecuencia para acceder a los servicios web informativos de la ESPOCH? Señale con una X desde el tipo de conexión menos utilizado hasta el más utilizado.

| | Nunca | Casi nunca | A veces | Casi siempre | Siempre |
|---|---|---|---|---|---|
| Wii – Fi (Internet casa) | | | | | X |
| Redes 2G | X | | | | |
| Redes 3G | X | | | | |
| Redes 4G | | | | | X |
| Internet publico | X | | | | |

**ANEXO F:** DIRECCIONAMIENTO DE LA RED SIMULADA.

| VLSM | | RED | MASCARAS | RANGO DE DIRECCIONES IP DISPONIBLES |
|---|---|---|---|---|
| **SERVIDORES** | | 192.168.1.0/24 | 255.255.255.0 | 192.168.1.1 - 192.168.1.254 |
| **SALUD** | | 192.168.2.0/24 | 255.255.255.0 | 192.168.2.1 - 192.168.2.254 |
| **MECÁNICA** | | 192.168.3.0/24 | 255.255.255.0 | 192.168.3.1 - 192.168.3.254 |
| **RECURSOS** | | 192.168.4.0/24 | 255.255.255.0 | 192.168.4.1 - 192.168.4.254 |
| **CIENCIAS** | | 192.168.5.0/24 | 255.255.255.0 | 192.168.5.1 - 192.168.5.254 |
| **PECUARIAS** | | 192.168.6.0/24 | 255.255.255.0 | 192.168.6.1 - 192.168.6.254 |
| **FADE** | | 192.168.7.0/24 | 255.255.255.0 | 192.168.7.1 - 192.168.7.254 |
| **FIE** | **LAB1** | 192.168.8.0/24 | 255.255.255.0 | 192.168.8.1 - 192.168.8.254 |
| | **LAB2** | 192.168.9.0/24 | 255.255.255.0 | 192.168.9.1 - 192.168.9.254 |
| | **LAB3** | 192.168.10.0/24 | 255.255.255.0 | 192.168.10.1 - 192.168.10.254 |
| | **LAB4** | 192.168.11.0/24 | 255.255.255.0 | 192.168.11.1 - 192.168.11.254 |
| | **LAB5** | 192.168.12.0/24 | 255.255.255.0 | 192.168.12.1 - 192.168.12.254 |
| | **LAB6** | 192.168.13.0/24 | 255.255.255.0 | 192.168.13.1 - 192.168.13.254 |
| | **LAB7** | 192.168.14.0/24 | 255.255.255.0 | 192.168.14.1 - 192.168.14.254 |
| **DTIC - FIE** | | 192.168.15.0/30 | 255.255.255.252 | 192.168.15.1 -192.168.15.2 |

| **DIRECCIONES IP DE LOS EQUIPOS** | | |
|---|---|---|
| **DTIC** | **e0/0** | 192.168.1.1/24 |
| | **e0/1** | 192.168.2.1/24 |
| | **e0/2** | 192.168.3.1/24 |
| | **e0/3** | 192.168.4.1/24 |
| | **e1/0** | 192.168.5.1/24 |
| | **e1/1** | 192.168.6.1/24 |
| | **e1/2** | 192.168.7.1/24 |
| | **s2/0** | 192.168.15.1/30 |
| **FIE** | **e0/0** | 192.168.8.1/24 |
| | **e0/1** | 192.168.9.1/24 |
| | **e0/2** | 192.168.10.1/24 |
| | **e0/3** | 192.168.11.1/24 |

| | | |
|---|---|---|
| | **e1/0** | 192.168.12.1/24 |
| | **e1/1** | 192.168.13.1/24 |
| | **e1/2** | 192.168.14.1/24 |
| | **s2/0** | 192.168.15.2/30 |

| **DIRECCIONES IP DE LAS COMPUTADORAS Y SERVIDORES** | | |
|---|---|---|
| **EQUIPO** | **DIRECCION IP** | **GATEWAY** |
| **PC_SALUD_1** | 192.168.2.10/24 | 192.168.2.1 |
| **PC_SALUD_2** | 192.168.2.20/24 | 192.168.2.1 |
| **PC_MECANICA_1** | 192.168.3.10/24 | 192.168.3.1 |
| **PC_MECANICA_2** | 192.168.3.20/24 | 192.168.3.1 |
| **PC_REC_1** | 192.168.4.10/24 | 192.168.4.1 |
| **PC_REC_2** | 192.168.4.20/24 | 192.168.4.1 |
| **PC_CIEN_1** | 192.168.5.10/24 | 192.168.5.1 |
| **PC_CIEN_2** | 192.168.5.20/24 | 192.168.5.1 |
| **PC_PEC_1** | 192.168.6.10/24 | 192.168.6.1 |
| **PC_PEC_2** | 192.168.6.20/24 | 192.168.6.1 |
| **PC_FADE_1** | 192.168.7.10/24 | 192.168.7.1 |
| **PC_FADE_2** | 192.168.7.20/24 | 192.168.7.1 |
| **PC_LAB1_1** | 192.168.8.10/24 | 192.168.8.1 |
| **PC_LAB1_2** | 192.168.8.20/24 | 192.168.8.1 |
| **PC_LAB2_1** | 192.168.9.10/24 | 192.168.9.1 |
| **PC_LAB2_2** | 192.168.9.20/24 | 192.168.9.1 |
| **PC_LAB3_1** | 192.168.10.10/24 | 192.168.10.1 |
| **PC_LAB3_2** | 192.168.10.20/24 | 192.168.10.1 |
| **PC_LAB4_1** | 192.168.11.10/24 | 192.168.11.1 |
| **PC_LAB4_2** | 192.168.11.20/24 | 192.168.11.1 |
| **PC_LAB5_1** | 192.168.12.10/24 | 192.168.12.1 |
| **PC_LAB5_2** | 192.168.12.20/24 | 192.168.12.1 |
| **PC_LAB6_1** | 192.168.13.10/24 | 192.168.132.1 |
| **PC_LAB6_2** | 192.168.13.20/24 | 192.168.13.1 |
| **PC_LAB7_1** | 192.168.14.10/24 | 192.168.14.1 |

| | | |
|---|---|---|
| **PC_LAB7_2** | 192.168.14.20/24 | 192.168.14.1 |
| **Sistema_web_institucional** | 192.168.1.100/24 | 192.168.1.1 |
| **MEDICINA** | 192.168.1.150/24 | 192.168.1.1 |
| **DTIC** | 192.168.1.200/24 | 192.168.1.1 |

**ANEXO G:** INSTALACIÓN DE JOOMLA.

yum update -y

yum install httpd mariadb-server php php-mysql php-curl php-gd php-pear php-memcache php-pspell php-snmp php-xmlrpc -y

systemctl start httpd ; systemctl enable httpd

systemctl start mariadb ; systemctl enable mariadb

mysql_secure_installation

Set root password? [Y/n] New password: <New_Strong_Password>

Re-enter new password: <New_Strong_Password>

Remove anonymous users? [Y/n] Y

Disallow root login remotely? [Y/n] Y

Remove test database and access to it? [Y/n] Y

Reload privilege tables now? [Y/n] Y

mysql -u root -p

Enter password:

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MariaDB connection id is 11

Server version: 5.5.52-MariaDB MariaDB Server

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database joomla_db;

Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> create user dbuser@localhost identified by 'Joomla@123#';

Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> grant all privileges on joomla_db.* to dbuser@localhost;

Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> flush privileges;

Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> exit

Bye

DESCARGAR JOOMLA DE LA PAGINA PRINCIPAL: https://downloads.joomla.org/

wget https://downloads.joomla.org/cms/joomla3/3-7-2/Joomla_3-7.2-Stable-Full_Package.zip

unzip Joomla_3-7.2-Stable-Full_Package.zip -d /var/www/html/

chown -R apache:apache /var/www/html/

chmod -R 775 /var/www/html/

systemctl restart httpd

firewall-cmd --permanent --add-service=http

firewall-cmd --permanent --add-service=https

firewall-cmd –reload

**ANEXO H:** CONFIGURACIÓN DE LA RED A SIMULAR.

DTIC

---

en

conf t

int e0/0

ip add 192.168.1.1 255.255.255.0

no sh

int e0/1

ip add 192.168.2.1 255.255.255.0

no sh

int e0/2

ip add 192.168.3.1 255.255.255.0

no sh

int e0/3

ip add 192.168.4.1 255.255.255.0

no sh

int e1/0

ip add 192.168.5.1 255.255.255.0

no sh

int e1/1

ip add 192.168.6.1 255.255.255.0

no sh

int e1/2

ip add 192.168.7.1 255.255.255.0

```
no sh
int s2/0
ip add 192.168.15.1 255.255.255.252
no sh
ip dhcp excluded-address 192.168.2.1
ip dhcp excluded-address 192.168.3.1
ip dhcp excluded-address 192.168.4.1
ip dhcp excluded-address 192.168.5.1
ip dhcp excluded-address 192.168.6.1
ip dhcp excluded-address 192.168.7.1
ip dhcp pool SALUD
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
ip dhcp pool MECANICA
network 192.168.3.0 255.255.255.0
default-router 192.168.3.1
ip dhcp pool RECURSOS
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
ip dhcp pool CIENCIAS
network 192.168.5.0 255.255.255.0
default-router 192.168.5.1
ip dhcp pool PECUARIAS
network 192.168.6.0 255.255.255.0
```

default-router 192.168.6.1

ip dhcp pool FADE

network 192.168.7.0 255.255.255.0

default-router 192.168.7.1

router eigrp 13

network 192.168.1.0

network 192.168.2.0

network 192.168.3.0

network 192.168.4.0

network 192.168.5.0

network 192.168.6.0

network 192.168.7.0

network 192.168.15.0

auto-summary

---

FIE

---

en

conf t

int e0/0

ip add 192.168.8.1 255.255.255.0

no sh

int e0/1

ip add 192.168.9.1 255.255.255.0

```
no sh
int e0/2
ip add 192.168.10.1 255.255.255.0
no sh
int e0/3
ip add 192.168.11.1 255.255.255.0
no sh
int e1/0
ip add 192.168.12.1 255.255.255.0
no sh
int e1/1
ip add 192.168.13.1 255.255.255.0
no sh
int e1/2
ip add 192.168.14.1 255.255.255.0
no sh
int s2/0
ip add 192.168.15.2 255.255.255.252
no sh
ip dhcp excluded-address 192.168.8.1
ip dhcp excluded-address 192.168.9.1
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.11.1
ip dhcp excluded-address 192.168.12.1
```

```
ip dhcp excluded-address 192.168.13.1

ip dhcp excluded-address 192.168.14.1

ip dhcp pool LAB1

network 192.168.8.0 255.255.255.0

default-router 192.168.8.1

ip dhcp pool LAB2

network 192.168.9.0 255.255.255.0

default-router 192.168.9.1

ip dhcp pool LAB3

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

ip dhcp pool LAB4

network 192.168.11.0 255.255.255.0

default-router 192.168.11.1

ip dhcp pool LAB5

network 192.168.12.0 255.255.255.0

default-router 192.168.12.1

ip dhcp pool LAB6

network 192.168.13.0 255.255.255.0

default-router 192.168.13.1

ip dhcp pool LAB7

network 192.168.14.0 255.255.255.0

default-router 192.168.14.1

router eigrp 13
```

network 192.168.8.0

network 192.168.9.0

network 192.168.10.0

network 192.168.11.0

network 192.168.12.0

network 192.168.13.0

network 192.168.14.0

network 192.168.15.0

auto-summary

---

PC_SALUD_1

---

ifconfig eth0 192.168.2.10 netmask 255.255.255.0

route add default gw 192.168.2.1 eth0

---

PC_SALUD_2

---

ifconfig eth0 192.168.2.20 netmask 255.255.255.0

route add default gw 192.168.2.1 eth0

---

PC_MECANICA_1

---

ifconfig eth0 192.168.3.10 netmask 255.255.255.0

route add default gw 192.168.3.1 eth0

---

PC_MECANICA_2

---

ifconfig eth0 192.168.3.20 netmask 255.255.255.0

route add default gw 192.168.3.1 eth0

---

PC_REC_1

---

ifconfig eth0 192.168.4.10 netmask 255.255.255.0

route add default gw 192.168.4.1 eth0

---

PC_REC_2

---

ifconfig eth0 192.168.4.20 netmask 255.255.255.0

route add default gw 192.168.4.1 eth0

---

PC_CIEN_1

---

ifconfig eth0 192.168.5.10 netmask 255.255.255.0

route add default gw 192.168.5.1 eth0

---

PC_CIEN_2

---

ifconfig eth0 192.168.5.20 netmask 255.255.255.0

route add default gw 192.168.5.1 eth0

---

PC_PEC_1

---

ifconfig eth0 192.168.6.10 netmask 255.255.255.0

route add default gw 192.168.6.1 eth0

---

PC_PEC_2

---

ifconfig eth0 192.168.6.20 netmask 255.255.255.0

route add default gw 192.168.6.1 eth0

---

PC_FADE_1

---

ifconfig eth0 192.168.7.10 netmask 255.255.255.0

route add default gw 192.168.7.1 eth0

---

PC_FADE_2

---

ifconfig eth0 192.168.7.20 netmask 255.255.255.0

route add default gw 192.168.7.1 eth0

---

PC_LAB1_1

---

ifconfig eth0 192.168.8.10 netmask 255.255.255.0

route add default gw 192.168.8.1 eth0

---

PC_LAB1_2

---

ifconfig eth0 192.168.8.20 netmask 255.255.255.0

route add default gw 192.168.8.1 eth0

---

PC_LAB2_1

---

ifconfig eth0 192.168.9.10 netmask 255.255.255.0

route add default gw 192.168.9.1 eth0

---

PC_LAB2_2

---

ifconfig eth0 192.168.9.20 netmask 255.255.255.0

route add default gw 192.168.9.1 eth0

---

PC_LAB3_1

---

ifconfig eth0 192.168.10.10 netmask 255.255.255.0

route add default gw 192.168.10.1 eth0

---

PC_LAB3_2

---

ifconfig eth0 192.168.10.20 netmask 255.255.255.0

route add default gw 192.168.10.1 eth0

---

PC_LAB4_1

---

ifconfig eth0 192.168.11.10 netmask 255.255.255.0

route add default gw 192.168.11.1 eth0

---

PC_LAB4_2

---

ifconfig eth0 192.168.11.20 netmask 255.255.255.0

route add default gw 192.168.11.1 eth0

---

PC_LAB5_1

---

ifconfig eth0 192.168.12.10 netmask 255.255.255.0

route add default gw 192.168.12.1 eth0

---

PC_LAB5_2

---

ifconfig eth0 192.168.12.20 netmask 255.255.255.0

route add default gw 192.168.12.1 eth0

---

PC_LAB6_1

---

ifconfig eth0 192.168.13.10 netmask 255.255.255.0

route add default gw 192.168.13.1 eth0

---

PC_LAB6_2

---

ifconfig eth0 192.168.13.20 netmask 255.255.255.0

route add default gw 192.168.13.1 eth0

---

PC_LAB7_1

---

ifconfig eth0 192.168.14.10 netmask 255.255.255.0

route add default gw 192.168.14.1 eth0

---

PC_LAB7_2

---

ifconfig eth0 192.168.14.20 netmask 255.255.255.0

route add default gw 192.168.14.1 eth0

**ANEXO I:** VULNERABILIDADES ENCONTRADAS CON OWASP ZAP.

ZAP Scanning Report

Summary of Alerts

| Risk Level | Number of Alerts |
|---|---|
| High | 1 |
| Medium | 3 |
| Low | 2 |
| Informational | 0 |

Alert Detail

| **High (Medium)** | **Cross Site Scripting (Reflejada)** |
|---|---|
| Description | Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology.<br><br>When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise.<br><br>There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based.<br><br>Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash.<br><br>Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any |

| | |
|---|---|
| | additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code. |
| URL | http://192.168.1.150/index.php/8-medicina?amp%3Btype=javascript%3Aalert%281%29%3B&format=feed |
| Method | GET |
| Parameter | amp;type |
| Attack | javascript:alert(1); |
| Evidence | javascript:alert(1); |
| URL | http://192.168.1.150/index.php/8-medicina?amp%3Bformat=javascript%3Aalert%281%29%3B&amp%3Btype=rss |
| Method | GET |
| Parameter | amp;format |
| Attack | javascript:alert(1); |
| Evidence | javascript:alert(1); |
| URL | http://192.168.1.150/?query=javascript%3Aalert%281%29%3B |
| Method | GET |
| Parameter | Query |
| Attack | javascript:alert(1); |
| Evidence | javascript:alert(1); |
| URL | http://192.168.1.150/index.php?amp%3Btype=javascript%3Aalert%281%29%3B&format=feed |
| Method | GET |
| Parameter | amp;type |
| Attack | javascript:alert(1); |
| Evidence | javascript:alert(1); |
| URL | http://192.168.1.150/index.php?amp%3Bformat=feed&amp%3Btype=javascript%3Aalert%281%29%3B |
| Method | GET |
| Parameter | amp;type |
| Attack | javascript:alert(1); |
| Evidence | javascript:alert(1); |
| URL | http://192.168.1.150/index.php?query=javascript%3Aalert%281%29%3B |
| Method | GET |
| Parameter | Query |
| Attack | javascript:alert(1); |
| Evidence | javascript:alert(1); |
| URL | http://192.168.1.150/index.php?amp%3Bformat=javascript%3Aalert%281%29%3B&format=feed&type=rss |
| Method | GET |
| Parameter | amp;format |
| Attack | javascript:alert(1); |
| Evidence | javascript:alert(1); |
| URL | http://192.168.1.150/index.php/8-medicina?amp%3Bformat=javascript%3Aalert%281%29%3B&format=feed&type=atom |
| Method | GET |
| Parameter | amp;format |
| Attack | javascript:alert(1); |

| | |
|---|---|
| Evidence | javascript:alert(1); |
| URL | http://192.168.1.150/index.php/8-medicina?amp%3Bformat=feed&amp%3Btype=javascript%3Aalert%281%29%3B |
| Method | GET |
| Parameter | amp;type |
| Attack | javascript:alert(1); |
| Evidence | javascript:alert(1); |
| URL | http://192.168.1.150/index.php?amp%3Bformat=javascript%3Aalert%281%29%3B&amp%3Btype=atom |
| Method | GET |
| Parameter | amp;format |
| Attack | javascript:alert(1); |
| Evidence | javascript:alert(1); |
| URL | http://192.168.1.150/index.php/8-medicina?query=javascript%3Aalert%281%29%3B |
| Method | GET |
| Parameter | query |
| Attack | javascript:alert(1); |
| Evidence | javascript:alert(1); |
| Instances | 11 |
| Solution | Phase: Architecture and Design<br><br>Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.<br><br>Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.<br><br>Phases: Implementation; Architecture and Design<br><br>Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.<br><br>For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.<br><br>Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed.<br><br>Phase: Architecture and Design |

| | |
|---|---|
| | For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.<br><br>If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.<br><br>Phase: Implementation<br><br>For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.<br><br>To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.<br><br>Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.<br><br>When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." |

| | |
|---|---|
| | Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere. |
| Reference | http://projects.webappsec.org/Cross-Site-Scripting<br><br>http://cwe.mitre.org/data/definitions/79.html |
| CWE Id | 79 |
| WASC Id | 8 |
| Source ID | 1 |

| **Medium (Medium)** | **Exploración de Directorios** |
|---|---|
| Description | Es posible ver el listado de directorios. La lista de directorios puede revelar scripts ocultos, incluyen archivos, copia de seguridad de los archivos de origen, etc, que se pueden acceder para leer información sensible. |
| URL | http://192.168.1.150/media/jui/js/ |
| Method | GET |
| Attack | Parent Directory |
| URL | http://192.168.1.150/media/jui/ |
| Method | GET |
| Attack | Parent Directory |
| URL | http://192.168.1.150/media/system/ |
| Method | GET |
| Attack | Parent Directory |
| URL | http://192.168.1.150/media/jui/css/ |
| Method | GET |
| Attack | Parent Directory |
| URL | http://192.168.1.150/media/system/js/ |
| Method | GET |
| Attack | Parent Directory |
| URL | http://192.168.1.150/templates/system/css/ |
| Method | GET |
| Attack | Parent Directory |
| Instances | 6 |
| Solution | Desactivar la exploración de directorios. Si esto es necesario, asegúrese de que los archivos de la lista no induce riesgos. |
| Reference | http://httpd.apache.org/docs/mod/core.html#options<br><br>http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html |
| CWE Id | 548 |
| WASC Id | 48 |
| Source ID | 1 |

| **Medium (Medium)** | **Buffer Overflow** |
|---|---|
| Description | Los errores de Buffer Overflow se caracterizan por la sobrescritura de espacios de memoria del proceso web en segundo plano, que no deberían haber sido modificados, intencionadamente o no. Sobrescribir los valores de IP (Instruction Pointer), BP (Base Pointer) y otros registros causan excepciones, violaciones del segmento y otros errores. Normalmente estos errores terminan la ejecución de la aplicación de manera inseperada. |

| | |
|---|---|
| URL | http://192.168.1.150/index.php/8-medicina?amp;format=feed&format=feed&type=atom |
| Method | GET |
| Parameter | type |
| Attack | GET http://192.168.1.150/index.php/8-medicina?amp%3Bformat=feed&format=feed&type=oFlIgFOcknUbwYKAldOTlUcwOZQHXfiufTcqovUwAaNofXDUTkiBAlxvdJWQmsUskoiUMqmlngdqIqOYQnjaSXiFtiWRHVlngexehvcWYotjcaRiYgGWlMgYyTrqAbGhBWXpxRdawcUxaqulkDphtbWvbaRdUqVMwyTvyLDFLKoYIfnLMJHYuXGamIgSickrUZvFmtSnMQndpsbTariAgRWWhnSvbVaBQYIDHevPsfOtmUmSwZcHXdsVGQCcWOvTOmlpwXIyapovRVtalCBqyecQqUxucvUAwPLkLdNOHHhqPkAKtYTvOctDbIrsAVVEDkHLJmmbboriBjivEeGXCJuixPTolZsTFXIqKaYeKgECHpMVoWTYjkeRQYVcaJluuTokoeiZnARBFXHCZdrmJXTPuGCJhaiKYTtKevQgSWaNweEIRwTBEWBvWlafUuYkQDHkoKTGgnWxQFDlQMPvpERxljyqLTEHbOmrMtkmhLuAudHvaspHeQZcQOketxicBlUtmAiEGQiqJxnPGihJWZNtgVXVIUtNSIfIHGOalFNXkTSDRFLObuTOnuEUehcQsETedRlZLNwJxhrDaMxWpZjmeXMfffFxMOqDhEnTWAgRSiLEbTqdWSnYmUVhInevyYfxyZUZWNAYpaYShPBTkuavwIyOeghGnFFXTKNscuGZyMghrLOkdohkMddHFsOQVXONfiWvZGrxbvkSBMXHGyqGeGxoFOiTJnHfyXPyUYOPaBEyIADZHmdFNLkPQrBZQsuWUlIBAPmhsIhkpcZrbpFAFymJbNOrqlDkxfECUJdVMbqkBmATiVEsmHxrXcXwvSSCjVTUicyVhjSZFgqayHwbAgakTZphLZYmeXNFsbbphNbhYKAsBGWQnjOlnccVwweigassHhKjqLZtfRQkmSNrHlmhICYEIMKeiumonLiOhjVQYSsRMGRKRACPidfTisTbImlmjIOVcHLMCeFEwgFkmVkLCdSXuscqrfqQYmfXdpApmpWVCBiZfvXkIiktxFWfPATpISPAwJNYnFhmABcDyqVueEJAyCpmSRkbhejnKFOuesqproyhamBCYKLPBbCLhNqXVXOnKeoHPFdpLrLTduhxJnYsqJRitAlpmvpqeNMhTyKDLTtxlkxWLspAULkmYHtIUGRDsjpqDYgxoQYRSxAPFTTqoofWPNolKWmgOOgwHOXZWvJqhmpdQUebgQdaHJTblGiGiCrcdXyAUjpuRDRCrbGlnEmvEPFNYbECOLxGlUAdtsmlepJVWVqSisXTlsaRsvCOyEATtGfgciwmpljZxCmpntjolgSJWwEOiWYDPiNsguxTlngZLfMjJCYHqqljPmxGtlAOMBNYQaPmvqoptXoFBWVkogobxlZwIrXObBwLWuAaGwqHBqkswoweLZqTqIxuqAPncLXxnZCXrggxBiMwERhNeqUGBQjIhJfbdovvZXqakDdXOoaRoqttqhHFfDuSHsedDMoeRUfUHktZMlGmZxZbHnZUWleAETTOCeStwSCuMFxaQBHPjnUNJrciUuNUaBCqNqpPeUjXZFDwZrciyPKlxIZiDrIQkaHMYNFBOoPkvnwHDcGQOhoUeAcjoOUyDwLpIXwecuFYdmgEvPTTUFtRpMSjKAxrdcNyUquNLGyMUwIRHcdgxjchPpXkseNpwggGKyqhjFooEcjAZiBokXSoarIUlJvHJciwIptmPfbIFkAPdNRGIpkoQBkmRjehyIkVIxYyQVtmaUFuSyhXbCcTqtaMjVNuCtAhYxlybYIVBtXYFUDHRPHmoOTMDGLXulvKWLopFvTiGemDRiAStMNnVIwKfXpswiiQCBORFPQpglEepCPejtBqbvWdqoyGgcXxmTeDSaGkUmXUZdeypOngIFtKnRgHnyATHTNuaCoHwrUChWqZZukkwqeTaXSjqtxxiOfyesOMTdCYYxSEYuCRrdqwkyqSrVZoQGJevbwJmXmAtEUSrZQsrfBfuJImYHDxsvLACnulSonuMkBvmNUGFRTjVQybSXAFMBTeOBaVlZAwAYpFFLLWdFtnXHPDQXPsMlSRlppkvSpiVoeBjZSUrqmmDmXOGMnxMmHdh HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0 Pragma: no-cache Cache-Control: no-cache Content-Length: 0 Referer: http://192.168.1.150/index.php/8-medicina?amp;format=feed&type=rss Cookie: 112c4b21f93ee408308cabc6581c2bf9=qpo7jr6n5226qocirmdqj1tt3h Host: 192.168.1.150 |

| | |
|---|---|
| URL | http://192.168.1.150/index.php/8-medicina?format=feed&type=atom |
| Method | GET |
| Parameter | type |
| Attack | GET http://192.168.1.150/index.php/8-medicina?format=feed&type=qxQsSHpfEVqsrjhWlDOZKboYqSlIxkQJZxqGNwSmNxkwnhGaSDMyfKLfENArgJgAQPOGPSEMysrinspZhxaglnRcYIoyidGUEAaWMWqaLhNJxbmvKaOGRlNwDUOTObagXsAporhUaFqMokXACvduXNiKrYlVwljwsUCwSqQFEbcNfRpTETDnLqOPEVtrtLrsVHJHoeZBXtdsVOiKRnCmNwsTTHSRkSWnbfptiPwFPypSrvDZihlNbrTvmAMQBqYWjyGTOlvHDDbZYKbjgDiZYgeYXwUxEtLNDdMjkRAfVXnfajbDCSvKKhFBNEvSTduQhNKHsptnyEbLstaUoDPYOGJHWCPEhndrEeCGXnldiJZgBiBsgNltUHDgfIbGWFaXfdXEnUnVPcRGCiiTqHadOeHcsQNLTkTWAwmEIpPdtCGWYrZcGhedeFtEQmFKWJVeiUsKCsrHPqcgkjXyMPNITMUNmTOYAeMJdXQpDGPDoKMAcYQZmZsEcBBIboMHFonDLphDyUioRcwgkSqhSElAbUMRZAYQXevQYtEIgvFZwcRQmKQKThJmTgBAFpvMHUUOrrdQTTsodAwEjVbBZGeKNEfiWlpIemctZcJDLkQyhwQfKnkcQvpoCylwNyEhOhYCopuZutKEipuXdZMZWGuFuKHtaBtlUUHeRrFWWFJjgnLcQjuMXoKwabofklvFVXUNtJXQJyJTuYQopQaPgpMhdLLuZvuyCGYQQiLhCcvanntSyanWYsZRHbJLAQOnECeWIFsoKGHcclVXsXeaBtMhhFgYMgqdxMpkyrjkfVvqFTrtpxYhbXjDrstvxuUCmysGgALWplXrGDVbiTISkUsXYOGjQAtfXmatkDcMVWtScdAskSIPVKjurXdCpxtEifViaPsufDKgeVdumBufOkHKWZwElaqWFWNeYNcUPkQFfVyxvWqGAWQhCJpnsRHCBEJmfjPIiuSXoOidBKJYiSeedYeXCwBXKRgCGxwHVSudbMmkEetUsfPGnqUobJnKiwxhsxNwNaQHuKnegbCGycdMqBEbWVytNbyLandyNNZCRxVocrkIPGDbaoVZeNRpOoXLsCTJmOrNPXyvnGZMgJAuUOcINjSrGJmZHPuXulotgpylFDAErbeOeRbfXtqGHjALdmYNrMnIWJTNnQBJgcqUGREtQAchsVMAnIotNljXIyoIBDRIimVnHCLoCfJAIIBQcmpElNIYZYxVqtGLxMogAohSZLSXKVoDIUyEVTrrweFghPwwGYRDZXIClqGgveLdJbMbyUlwCbatLyWqdmjTTTgTTKXikbVvmPwQnnjreolpwqFQApkoEscCNqmbDnQYfvpyRdHUgdrAsqSksJIQHShxAGumtPoxDFUNnFKZVoyCwlNHgdkKbBQNcabxfsHAcJoHoYbtdWiTPjcKJddurXmGfdBaYlaSfAXEwRXUkuWGgoPfhLYZJYFNrKvDgiiwfWyrWMrNjJHbiQmIrgjDKupyAYqhQcIVgYCVnDiJWsshPBtMYcEUyUyrjRSohacepEgKhsvALbVqYeLbyrweRNjKjqPdRbINVKkRviDmukpQmlVXRbQdgGFBMeFnRVhfjSYCJkZvYtyyJOaRjGBryukUGSmbyxFMfyRNOrlvhfIFpDeLGbcJgLIIjEgaIZwgjXwIVDWexhxqZvKRMeAoSpNNUTdjRvjrUKWtfVQPjTADmCdtKSaHbcpRdhSNDYFlmIMYqEljZqtRiTDGjdtklIFrVEdtNyCvMRiKbsLKkLeLamYFbaAgnOfVkmyCiMoCxlwnRvMIGlHxNvQiFGmnjOgwZUANlHneLWjgNQtXbEmCpmqWXsiqoarbatlWDYsQSOthqFjHNLCcKfHcsgGfeBeEUSkJjfjPYdwgiLwpAdlIQtvdpROPIRLLDUxqqtiebalRumbPdqWOYrOpGRyUfgfsxnQNfAEsxJPggVSojqDfYskQEuTRhtqpJkVsneMhiUZfqgRucaiaewLnYIDFsuITacpZQJVlZVmsqiyOkkfZewYbQLwBabUWjtIEIHDUPOIvpagBiWaZHxOpeQqqTQSirdlBAVVZnvFAsSxeEBcrkKeDOVjm HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0 Pragma: no-cache Cache-Control: no-cache Content-Length: 0 Referer: http://192.168.1.150/index.php/8-medicina Cookie: 112c4b21f93ee408308cabc6581c2bf9=qpo7jr6n5226qocirmdqj1tt3h Host: 192.168.1.150 |
| URL | http://192.168.1.150/index.php?amp;format=feed&format=feed&type=rss |
| Method | GET |

| Parameter | type |
| --- | --- |
| Attack | GET http://192.168.1.150/index.php?amp%3Bformat=feed&format=feed&type=byyKmGoPsRyopcmZECANWAvoqlxGMeXstwsnBWmWcNQxklkMJXqHpxKYRASZmEQKfVSYJhxhbClECnWAcqtQQISklRnRXcKUcXmULSWaiABpeNvMIKbukYvGnJZmCGUGfJldEJEOQEWTtjjFIpnhjBcIoBmVvepsNlJXaGWSktXZARiUyegpfCIcDutkNIujqosisKoNhULgwvVPVvhWemylHRgZHdkCpqWbXPnhmBQBglUSgPfVCJuGTaZsokYHffXmfOUDmXNdxuZDEfJQfKAPrcqoGFqvZxCPtmGhRKieonrEIEgWRXgNyqQfScjNKTuubvWkpagAEUEUKBTvdmfflQhBmIWEiCgqCTZDuMYSteHcSeXGrFmklYBonUvaRclLtFQyXTaQJGGyhUeWTBqlChgokBxokBnNvIxFJiZEYTNbWZRxJLFxhYjKMIvJltjiWKGVxyqOESKrWdwxovWksmilxrMcyXTSLMcNxdcZIVfocHWmjNanAfoxhdKTpphVmsuTGoBiBvbcKiqTroeivRFQuurLnpJsKguFFxCDPqolQhrcylJLDFRdSjenIVTgBrsFufKAdJZVGlenvHyOHsGrlgdIruAkflXKcPQLtkqBPcTjYZpPEvfiEOZSOKLCOcSpUZXlZJtwuQDXEBYxmTSrcSRWVUTJZZngEeGQeAoCKYNKdlLkLJxPDLWhtydYkPEerXwlItnkJJSYsWvqQOmPDyLPXLrHnQwmybWyvQlVeGikrZjjvWYkPunQZffPDvZcKVaXKbOjGqCuftuonLdErBelaRqdVLSfdofDhtyenHjQRKqrVZwTEDSRbcoJOeMElRIFYaoXFVWSHxvydMdbmyjCcxbVwcNtwlHtLSsguZaxhxhoHQsQuoTLwMWCByefXXxxajSHoKMUtvVsAWraNrEFVLNFOiFSwZrOnkUdWsKbOIkoqVpaCYRpYTdrPtEEBnvLjiURPOsmJEOMUUKdZhJVleDkVgSQROswKmDvEEXlEhFnslQDMOrpseEOrJryNkKCZnaYrqOminaPyTgolXPIdfIUbHuiLTUJidAZSuteoTTreuGQMSSESZcPCqHtSBDmFPXUTgQwejKIgWlIdygMVSsDxGUTYqVOWPDqHymaTSKGhBRjtwKwDKcIGDaMDotUkvBnjnQSIJqGgjcSdEtJyLBniaAXcvjCLflbRwMyhqhIcweAsjmwLLZOCYehSgDFSuwPMoqOkciInNolRUstPMpkeSgHbOcluXnLcepEjcVvkAwvqUlebiOLUwHajmVkOusSLnDFuteMUNQsAOsHJrvVhVvcAFXkacmRawQmOtfjcwKSmukfnXxYqlJfHpBIyDoboWZhxFLOjJjqIJnjHtLXnGSjKOjZMXsbAxDDBWwuTByWsFPAdGIVWsAeurvqvYDSbPTRQrNUuNJVjdShCcZYdiBXZPAlZnPANIkdkLlWfYeIrDSdRZleUkiWWtsFscVPvPsPuxWilxSHuDdywMyrHjadJnKfXWgIxqYFwYrBpNyVBiJjsNQjZjEvujtOcxSJPhvPuVxbNrJLXuNwUoTNOlAJbBWoXhLlZbcYPMmvPmkVeMVXjgLuunOSHovEkvcIDdJIpYbWAbojnZjTZkRGrlVypjkPuNfSqlhTpLTTwFYwjXZVelOwYmYEDpbuZONAcccLHxFNeayAicgBACZFrCWVfvNpbhsdLFRLoZapKaEPHSYsBOgQMlHKSiTyWyytNZPgrljFhsxhckbZDlhNjdbufgoHcRKWNwuoOwKDxsVSoMDQimqLESixURiruxpMxPFfPNhjsUtQVSjpfYIrWsRQNWZtFuWArwuZhBrVvRRBDCxbyuAVGQoJgZeFpwfGSJjLuDilTUgWaclBRRbMGVMIZspLeGyibAPAYUDUNojwggtFamVDruYImENiAooSYwXruQdibiTEYecIhRmbFHlsjEbdgCBPoCLLZjibuYvlqToKseuZelXOtDOTecnHUsxxZvhqfkYaNwAOKqFQRecIUtkcmPWDdWXXylaKEkTnEsOsZLiGoIyZwKDqmclaFjCCrWDWJRTYiHkSBQDapqOsNClnSsoEJvUp HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0 Pragma: no-cache Cache-Control: no-cache Content-Length: 0 Referer: http://192.168.1.150/index.php?amp;format=feed&type=atom&type=rss Cookie: 112c4b21f93ee408308cabc6581c2bf9=qpo7jr6n5226qocirmdqj1tt3h Host: 192.168.1.150 |
| URL | http://192.168.1.150/index.php?format=feed&type=atom |
| Method | GET |

| Parameter | type |
| --- | --- |
| Attack | GET http://192.168.1.150/index.php?format=feed&type=eyOpGxBsNhEoIheNCrLgiOdHFmlHBUXfnJkGcNyhadTMCQvqkepkBhUsdydAhvCTxaRuLwITCfiMtUPjcAYoDwPXRUAFCjSUJhKErVMJnZRqwpFubYnEjImcCYCRHKJJXReWXhTuhLuMknaTrLertJmfpiQGZymmCUhjcRXZBfSIkiNBmVBnDFSqjZpDAEBcSbIaVVkcCfJBdhNpTOtSmukPkduWMioPQdIQULxqEwOcXPIkelvMtbtPAKjmZwKipAiLqQGXQVhakmVjyHsNLIAYVJNMHrAvMCnVWIQWGRYXprGfxheAltsapYxAhKGLNgPojNGjxxbWFQQHghkRdslIRddGECEOJQqNjWtXOYFYIEJKRTDmCXFZAqrYDVikJVkKJbOBPmmZHgJCFDLTaiICJDnsgavxfBJWyrLPkuEIpVUcBkWkwyIAAEhYhHdcSeWKnhZFWcdnxQYxFjmYroWBtyjqtPAgfeogIkFsDOZKGPyDDsAInXBKNuDgebroqVwRgigYlaadfDlIyCAypmJfesWcLAABIVLqGXirxGjrFBvnmgKLgkPFoBaARrfTwTUnLlnGfCqmvVGZuvsKKLWJFXCjeBpZgqfAegDySgyvUEaNeQSXNmWnvvARTprfwoZceQEbljNcJBNaeHRIkEgMwjNybbTuuydjrxcnxJgjFkpeWRiNiylaOFAeNMDoZdYomggyIqAnLmiGtCQTgLrHrSwTWTyhSScnxpWfOipKvVtaTwcyyDOgjYPiAKFYCgWJVOanMVBebihWBAkQjPxccOunkseDSQdNwHslocjhCEFCnwytehbEtfvdhENHZRXevWZbYwdJJDuanEtSFQpdximQVBtwYPPZCukuQUnvBeowiSigBkEUPNGUGrViBvxefBsXlucAvpAvvQoIMPVYYGakbObcCJPAbsMGjKWMyyyxKKBOBQmIhTTiuUEkbstbfYBwKiMKtcBluiGYGYnRxwFwxkQYHNVRApOpggHjvGvbHCBawgNuYfluaLengpWJuPFmtETNYneKxorbSRwixwSCfcRRapTtMXYHHWTmqbWYPBACArLaPbSISUIfrmNpVjyjrwnFWTNYZrZbFunyapjCDZAnaGuKBKlHvUtGOvZGEDxhvbNeQFEROdSUiyAZJVoIsNpfUraVXfvdsDaTYyANbwWsCeVbNicsKXpAFSEGQAkUvMckHnejEHHClaGRYnOSWRbpWDOhRvjnXhhVhQsViJuTHnVZkOsNCwTiYNmcBLliCvVOvPvnynygwhduFTccNKmlXInQwMjXynOwYnEARaeCZplQbBxkFamdtGyvxdbwvNwUiCAKHktGEotNptnESoOTCkAuJuMVSwTfVnIArXGUNlGNLVgbBMvryosOeAdqCEwdBdbXCZygIMXOPZKgOQWlflwDEynggOHHDgYtqFPHXSpOcXdjEdtShaDuGiLWhcPxZKZrvQNlRPrbrMLajUbZtoZsngtekNnbYgnFhisNNoumJRcGVKSbHksdVaCkOMNSMruETLWWrVxgXWmKNGRfkDQRELMvugqVxxCCNcqByVYAleaFFMKScOplRKMPDDEcIsQBCjjVXHTNrcpHQQoWmwRElJFmNnPUkUUNOephGDrXtVioHsgAKQiyliAkOxKKmoiolEuFARshggXdNMeuCNsGvpmFyBlnAaammSNrUAjiRMbLbHcnMUKEWgNUywYFcPuXgrIVxelybxBsSIuZDNWbVjSsoNsULpdrdYdldcDFeJDwQFqmjSiTRVkUdfdpJjucevdQhDOAxBvKMDlIYyrcjjtdQvGZFALkIcdHxiblxSjupacbuFEHvRaDrHTTXRYuNqNqbJdQQwXXBItUxJiVnEhZFxjSfxuUoKNBewpJRKqhGDwqcwBAGRLHLcErsbFvBCscsuGREvAcajCYxeUTJbHqQSDqsujpsOYPSboomEQZdVwIWbIXEnDgVcdtXqCpRhrWeMhEDvAbxGZhSxevVaBvLdiepoKsQZPIyJdlQlldpxgmmcrfDMPGxkeSTxZFZsPHwbGbpJDUgAKrWbrKRuvTdNQonLFIipuEgVCYMMQbWttGSiLauqSm HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0 Pragma: no-cache Cache-Control: no-cache Content-Length: 0 Referer: http://192.168.1.150 Cookie: 112c4b21f93ee408308cabc6581c2bf9=qpo7jr6n5226qocirmdqj1tt3h Host: 192.168.1.150 |
| Instances | 4 |
| Solution | Reescribir el programa en segundo plano realizando una correcta comprobación de la longitud de retorno. Esto requerirá el recompilado del ejecutable en segundo plano. |

| | |
|---|---|
| Other information | Potencial desbordamiento de buffer. El script ha cerrado la conexión y ha lanzado un error interno del servidor 500 |
| | |
| Reference | https://www.owasp.org/index.php/Buffer_overflow_attack |
| CWE Id | 120 |
| WASC Id | 7 |
| Source ID | 1 |
| **Medium (Medium)** | **Encabezado X-Frame-Options no establecido** |
| Description | El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'. |
| URL | http://192.168.1.150/index.php/8-medicina/1-medicina?print=1&tmpl=component |
| Method | GET |
| Parameter | X-Frame-Options |
| URL | http://192.168.1.150/index.php?amp;format=feed&type=atom&type=rss |
| Method | GET |
| Parameter | X-Frame-Options |
| URL | http://192.168.1.150/index.php/8-medicina?amp;format=feed&type=atom&type=rss |
| Method | GET |
| Parameter | X-Frame-Options |
| URL | http://192.168.1.150/index.php?amp;format=feed&type=atom |
| Method | GET |
| Parameter | X-Frame-Options |
| URL | http://192.168.1.150/index.php |
| Method | GET |
| Parameter | X-Frame-Options |
| URL | http://192.168.1.150/index.php/8-medicina/1-medicina |
| Method | GET |
| Parameter | X-Frame-Options |
| URL | http://192.168.1.150 |
| Method | GET |
| Parameter | X-Frame-Options |
| URL | http://192.168.1.150/ |
| Method | GET |
| Parameter | X-Frame-Options |
| URL | http://192.168.1.150/index.php/8-medicina?amp;format=feed&type=rss |
| Method | GET |
| Parameter | X-Frame-Options |
| URL | http://192.168.1.150/index.php/8-medicina |
| Method | GET |
| Parameter | X-Frame-Options |
| URL | http://192.168.1.150/index.php?amp;format=feed&type=rss |
| Method | GET |
| Parameter | X-Frame-Options |
| Instances | 11 |

| | |
|---|---|
| Solution | Los navegadores de web más modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras formas si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles). |
| Reference | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx |
| CWE Id | 16 |
| WASC Id | 15 |
| Source ID | 3 |
| **Low (Medium)** | **No se encuentra encabezado X-Content-Type-Options Header** |
| Description | El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. |
| | |
| URL | http://192.168.1.150/index.php?amp;format=feed&format=feed&type=atom |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/templates/system/css/system.css |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/index.php/8-medicina?amp;format=feed&type=atom&type=rss |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/index.php/8-medicina?amp;type=rss&format=feed |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/index.php?amp;format=feed&format=feed&type=rss |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/index.php/8-medicina/1-medicina?print=1&tmpl=component |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/media/jui/css/bootstrap.min.css |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/index.php/8-medicina?format=feed&type=rss |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/templates/system/css/general.css |

| | |
|---|---|
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/templates/ok_nemesis/js/uikit.min.js |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/templates/ok_nemesis/js/extras.js |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/index.php?amp;format=feed&type=atom |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/templates/ok_nemesis/css/ok-animation.css |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/templates/ok_nemesis/css/bootstrap.css |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/index.php?amp;type=atom&format=feed |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/images/1.jpg |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/media/jui/css/bootstrap-extended.css |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/media/system/js/caption.js?1333706ec52f6008e680fe5e0515a58c |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/ |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://192.168.1.150/templates/ok_nemesis/js/orionkit.js |
| Method | GET |
| Parameter | X-Content-Type-Options |
| Instances | 46 |
| Solution | Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.<br><br>Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. |
| Other information | Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de |

| | |
|---|---|
| | contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. |
| Reference | http://msdn.Microsoft.com/en-us/library/Ie/gg622941%28v=vs.85%29.aspx<br>https://www.owasp.org/index.php/List_of_useful_HTTP_headers |
| CWE Id | 16 |
| WASC Id | 15 |
| Source ID | 3 |

| **Low (Medium)** | **Protección de buscador de web XSS no disponible** |
|---|---|
| Description | La protección del buscador de web XSS no está disponible, o está deshabilitada por la configuración de la cabecera de respuesta de HTTP 'X-XSS-Protection' en el servidor de web |
| | |
| URL | http://192.168.1.150/index.php/8-medicina?amp;format=feed&type=rss |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/images/2.jpg" |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/index.php |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/index.php/8-medicina?amp;format=feed&type=atom&type=rss |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/index.php?amp;format=feed&type=atom |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/index.php/8-medicina |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150 |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/index.php?amp;format=feed&type=atom&type=rss |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/index.php/8-medicina/1-medicina |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/templates/ok_nemesis/css/nemesis.css |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/images/3.jpg" |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/index.php?amp;format=feed&type=rss |

| | |
|---|---|
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/images/1.jpg" |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/index.php/8-medicina/1-medicina?print=1&tmpl=component |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/robots.txt |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/sitemap.xml |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://192.168.1.150/ |
| Method | GET |
| Parameter | X-XSS-Protection |
| Instances | 17 |
| Solution | Asegúrese que el filtro XSS del navegador web está habilitado, estableciendo el encabezado de respuesta HTTP X-XSS-Protection en '1'. |
| Other information | El encabezado de respuesta HTTP X-XSS-Protection le permite al servidor web habilitar o deshabilitar el mecanismo de protección del navegador web XSS. Los siguientes valores intentan habilitarlo:<br><br>X-XSS-Protection: 1; mode=bloqueo<br><br>X-XSS-Protection:1; reporte=http://www.example.com/xss<br><br>Los siguiente valores lo deshabilitarían:<br><br>X-XSS-Protection: 0<br><br>El encabezado de respuesta HTTP X-XSS-Protection es actualmente compatible en Internet Explorer, Chrome y Safari (WebKit). Tenga en cuenta que esta alerta solo se produce si el cuerpo de respuesta podría pontecialmente contener una carga útil XSS (con un tipo de contenido basado en texto, con una longitud distinta de cero). |
| Reference | https://www.OWASP.org/index.php/XSS _ (Cross_Site_Scripting) _Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/ |
| CWE Id | 933 |
| WASC Id | 14 |
| Source ID | 3 |

**ANEXO J:** INSTALACIÓN Y EJECUCIÓN DEL ATAQUE DDOS SYN CON SLOWLORIS.

En la maquina de Kali Linux descargar el archivo con el siguiente comando:

git clone https://github.com/llaera/slowloris.pl.git

cd slowloris.pl

Para analizar los puertos se utiliza el siguiente comando:

nmap (Direccion IP del servidor victima)

perl slowloris.pl -dns (Dirección IP del servidor victima) –port (Puerto abierto por lo general 80) –time (Tiempo) –num (Número de paquetes) –cache

**ANEXO K:** CANTIDAD DE PAQUETES REGISTRADOS POR EL GRUPO DE INVESTIGACIÓN SEGINTE.

| Fecha | Paquetes. Recibidos |
|---|---|
| 15 de Mayo | 649207734 |
| 16 de Mayo | 749684523 |
| 17 de Mayo | 694793613 |
| 18 de Mayo | FIN DE SEMANA |
| 19 de mayo | |
| 20 de Mayo | 734297481 |
| 21 de Mayo | Problema |
| 22 de Mayo | Problema |
| 23 de Mayo | 773498541 |
| 24 de Mayo | Feriado |
| 25 de Mayo | FIN DE SEMANA |
| 26 de Mayo | |
| 27 de Mayo | 742097705 |
| 28 de Mayo | 750945494 |
| 29 de Mayo | 838064475 |
| 30 de Mayo | 631401534 |
| 31 de Mayo | 1374642056 |
| 1 de Junio | FIN DE SEMANA |
| 2 de Junio | |
| 3 de Junio | 1000654319 |
| 4 de Junio | 787606614 |
| 5 de Junio | 877280028 |
| 6 de Junio | 676079237 |
| 7 de Junio | 135966421 |
| 8 de Junio | FIN DE SEMANA |
| 9 de Junio | |
| 10 de Junio | Problema |
| 11 de Junio | 716205127 |
| 12 de Junio | 444123232 |
| 13 de Junio | 496610887 |
| 14 de Junio | 1276613488 |
| 15 de Junio | FIN DE SEMANA |
| 16 de Junio | |
| 17 de Junio | 635590275 |
| 18 de Junio | 1218596770 |
| 19 de Junio | |
| 20 de Junio | 669847042 |
| 21 de Junio | 1185732117 |
| 22 de Junio | FIN DE SEMANA |
| 23 de Junio | |

| | |
|---|---|
| 24 de Junio | 651908738 |
| 25 de Junio | 641683132 |
| 26 de Junio | 686294023 |
| 27 de Junio | 580804867 |
| 28 de Junio | 1122656857 |
| 29 de Junio | FIN DE SEMANA |
| 30 de Junio | |
| 1 de Julio | 452206640 |

**ANEXO L:** EJECUCIÓN DEL ATAQUE DDOS SYN CON METASPLOIT.

Abrir Metasploit que viene por defecto en Kali Linux

search synflood

use auxiliary/dos/tcp/synflood

set rhost (Dirección IP del servidor victima)

set timeout (Tiempo)

set num (Número de paquetes, no es necesario)

show options

exploit

**ANEXO M:** TIEMPOS DE DENEGACIÓN Y RECUPERACIÓN DE LOS SERVICIOS WEB INFORMATIVOS DE MEDICINA, DTIC Y SISTEMA ACADÉMICO RESPECTIVAMENTTE.

| | **MEDICINA** | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en realizar la denegación)** | **Metasploit(Tiempo se demora en realizar la denegación)** |
| 649207734 | 97.52 | 894.89 |
| 749684523 | 80.05 | 844.14 |
| 694793613 | 113.78 | 909.4 |
| 734297481 | 97.78 | 640.86 |
| 773498541 | 76.09 | 629.87 |
| 742097705 | 85.68 | 807.91 |
| 750945494 | 87.79 | 898.85 |
| 838064475 | 66.98 | 745.23 |
| 631401534 | 68.87 | 902.57 |
| 1374642056 | 54.79 | 692.44 |
| 1000654319 | 61.43 | 792.12 |
| 787606614 | 81.43 | 883.3 |
| 877280028 | 71.02 | 838.58 |
| 676079237 | 95.83 | 879.78 |
| 135966421 | 168.34 | 1448.61 |
| 716205127 | 70.51 | 850.83 |
| 444123232 | 227.33 | 1148.08 |
| 496610887 | 198.35 | 1058.63 |
| 1276613488 | 57.49 | 816.7 |
| 635590275 | 98.54 | 909.73 |
| 1218596770 | 52.77 | 884.23 |
| | 51.24 | 872.56 |
| 669847042 | 96.12 | 1091.87 |
| 1185732117 | 63.59 | 741.52 |
| 651908738 | 99.4 | 895.93 |
| 641683132 | 92.35 | 965.15 |
| 686294023 | 103.65 | 906.54 |
| 580804867 | 143.57 | 1015.56 |
| 1122656857 | 68.66 | 831.98 |
| 452206640 | 214.27 | 1093.62 |

| | MEDICINA | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en recuperarse de la denegación)** | **Metasploit(Tiempo se demora en recuperarse de la denegación)** |
| 649207734 | 24.02 | 30.83 |
| 749684523 | 28.46 | 28.24 |
| 694793613 | 22.89 | 21.03 |
| 734297481 | 14.33 | 20.12 |
| 773498541 | 22.77 | 31.55 |
| 742097705 | 18.59 | 33.64 |
| 750945494 | 15.54 | 38.54 |
| 838064475 | 31.1 | 31.12 |
| 631401534 | 33.24 | 30.13 |
| 1374642056 | 56.78 | 40.13 |
| 1000654319 | 15.47 | 39.56 |
| 787606614 | 35.07 | 45.01 |
| 877280028 | 30.01 | 26.89 |
| 676079237 | 17.26 | 24.89 |
| 135966421 | 18.68 | 22.56 |
| 716205127 | 29.58 | 30.12 |
| 444123232 | 17.67 | 18.26 |
| 496610887 | 27.47 | 22.71 |
| 1276613488 | 17.44 | 20.15 |
| 635590275 | 31.18 | 28.95 |
| 1218596770 | 17.73 | 32.56 |
| | 17.79 | 29.13 |
| 669847042 | 19.33 | 20.69 |
| 1185732117 | 29.97 | 25.41 |
| 651908738 | 18.12 | 20.27 |
| 641683132 | 30.24 | 28.53 |
| 686294023 | 25.3 | 26.54 |
| 580804867 | 19.82 | 21.89 |
| 1122656857 | 30.86 | 25.64 |
| 452206640 | 19.67 | 18.52 |

| | DTIC | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en realizar la denegación)** | **Metasploit(Tiempo se demora en realizar la denegación)** |
| 649207734 | 182.56 | 873.5 |
| 749684523 | 92.68 | 820.14 |
| 694793613 | 127.91 | 889.45 |
| 734297481 | 87.31 | 804.21 |
| 773498541 | 98.62 | 908.38 |
| 742097705 | 95.05 | 881.52 |
| 750945494 | 104.54 | 969.53 |
| 838064475 | 77.74 | 720.98 |
| 631401534 | 55.25 | 884.87 |
| 1374642056 | 71.25 | 700.54 |
| 1000654319 | 69.73 | 788.21 |
| 787606614 | 94.87 | 879.85 |
| 877280028 | 74.43 | 811.13 |
| 676079237 | 89.76 | 832.56 |
| 135966421 | 193.39 | 1503.68 |
| 716205127 | 72.62 | 856.78 |
| 444123232 | 153.98 | 1105.72 |
| 496610887 | 97.83 | 1028.34 |
| 1276613488 | 92.8 | 801.27 |
| 635590275 | 111.72 | 964.63 |
| 1218596770 | 62.53 | 839.51 |
| | 69.77 | 936.72 |
| 669847042 | 129.41 | 1128.93 |
| 1185732117 | 92.61 | 798.21 |
| 651908738 | 92.98 | 902.56 |
| 641683132 | 71.27 | 978.36 |
| 686294023 | 83.1 | 956.21 |
| 580804867 | 126.65 | 1120.75 |
| 1122656857 | 85.17 | 850.39 |
| 452206640 | 198.59 | 1167.82 |

| | DTIC | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en recuperarse de la denegación)** | **Metasploit(Tiempo se demora en recuperarse de la denegación)** |
| 649207734 | 27.85 | 24.14 |
| 749684523 | 21.37 | 31.03 |
| 694793613 | 21.95 | 22.87 |
| 734297481 | 25.94 | 24.35 |
| 773498541 | 24.51 | 27.14 |
| 742097705 | 20.73 | 28.64 |
| 750945494 | 20.61 | 33.51 |
| 838064475 | 28.52 | 26.18 |
| 631401534 | 21.08 | 26.37 |
| 1374642056 | 20.6 | 32.19 |
| 1000654319 | 20.87 | 37.57 |
| 787606614 | 20.3 | 41.05 |
| 877280028 | 21.89 | 29.64 |
| 676079237 | 19.12 | 26.38 |
| 135966421 | 35.23 | 27.59 |
| 716205127 | 20.02 | 23.1 |
| 444123232 | 33.74 | 26.94 |
| 496610887 | 19.95 | 23.58 |
| 1276613488 | 22.88 | 21.45 |
| 635590275 | 24.4 | 22.93 |
| 1218596770 | 19.81 | 26.47 |
| | 21.08 | 24.51 |
| 669847042 | 20.99 | 21.54 |
| 1185732117 | 22.63 | 21.96 |
| 651908738 | 20.13 | 22.05 |
| 641683132 | 19.13 | 22.83 |
| 686294023 | 19.87 | 21.74 |
| 580804867 | 20.31 | 22.54 |
| 1122656857 | 21.15 | 23.49 |
| 452206640 | 25.98 | 22.87 |

| | SISTEMA WEB ACADÉMICO | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en realizar la denegación)** | **Metasploit(Tiempo se demora en realizar la denegación)** |
| 649207734 | 174.92 | 865.17 |
| 749684523 | 75.24 | 854.29 |
| 694793613 | 77 | 900.23 |
| 734297481 | 104.9 | 876.51 |
| 773498541 | 85.04 | 915.49 |
| 742097705 | 104.58 | 862.05 |
| 750945494 | 78.36 | 925.83 |
| 838064475 | 85.89 | 768.91 |
| 631401534 | 54.29 | 921.87 |
| 1374642056 | 73.93 | 695.26 |
| 1000654319 | 80.47 | 809.03 |
| 787606614 | 115.68 | 896.14 |
| 877280028 | 95.05 | 845.6 |
| 676079237 | 112.61 | 866.02 |
| 135966421 | 186.22 | 1486.93 |
| 716205127 | 110.65 | 845.23 |
| 444123232 | 152.46 | 1129.94 |
| 496610887 | 75.87 | 1072.36 |
| 1276613488 | 75.8 | 826.01 |
| 635590275 | 148.33 | 954.86 |
| 1218596770 | 77.01 | 874.12 |
| | 74.86 | 915.3 |
| 669847042 | 91.47 | 1135.03 |
| 1185732117 | 83.63 | 815.2 |
| 651908738 | 127.1 | 921.57 |
| 641683132 | 134.38 | 984.13 |
| 686294023 | 149.11 | 943.31 |
| 580804867 | 71.94 | 1098.52 |
| 1122656857 | 94.09 | 875.49 |
| 452206640 | 77.17 | 1145.97 |

| | SISTEMA WEB ACADÉMICO | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en recuperarse de la denegación)** | **Metasploit(Tiempo se demora en recuperarse de la denegación)** |
| 649207734 | 35.71 | 27.51 |
| 749684523 | 30 | 29.63 |
| 694793613 | 31.44 | 25.1 |
| 734297481 | 19.88 | 23.72 |
| 773498541 | 30.97 | 29.35 |
| 742097705 | 31.38 | 32.67 |
| 750945494 | 20.25 | 30.21 |
| 838064475 | 19.8 | 28.1 |
| 631401534 | 32.07 | 29.36 |
| 1374642056 | 30.95 | 35.12 |
| 1000654319 | 34.92 | 35.19 |
| 787606614 | 19.98 | 39.74 |
| 877280028 | 31.84 | 28.39 |
| 676079237 | 25.17 | 28.07 |
| 135966421 | 34.97 | 26.41 |
| 716205127 | 19.33 | 28.54 |
| 444123232 | 21 | 25.93 |
| 496610887 | 31.9 | 26.78 |
| 1276613488 | 32.26 | 24.88 |
| 635590275 | 30.06 | 27.19 |
| 1218596770 | 21.89 | 30.61 |
| | 20.23 | 28.06 |
| 669847042 | 20.08 | 23.97 |
| 1185732117 | 19.13 | 24.13 |
| 651908738 | 20.46 | 25.09 |
| 641683132 | 32.06 | 27.67 |
| 686294023 | 31.46 | 23.22 |
| 580804867 | 31 | 24.05 |
| 1122656857 | 20.29 | 22.13 |
| 452206640 | 31.3 | 26.91 |

**ANEXO N:** INSTALACIÓN Y CONFIGURACIÓN DE MOD_QOS

yum install openssl-devel.x86_64

yum install pcre-devel.x86_64

yum install httpd-devel.x86_64

Descargar mod de la siguiente dirección: https://www.mediafire.com/file/i35mnrrgzvc5mxk/mod_qos-10.15.tar.gz/file

Descomprimimos:

tar -zxvf mod_qos-10.15.tar.gz

cd mod_qos-10.15

cd apache2

apxs -i -c  mod_qos.c

Se edita el archivo:

vim /etc/httpd/conf/httpd.conf

Insertando al final del archivo el siguiente código para el módulo_qos:

LoadModule qos_module /usr/lib64/httpd/modules/mod_qos.so

Se crea el archivo de configuración con nombre mod_qos.conf:

touch /etc/httpd/conf.d/qos.conf

vim /etc/httpd/conf.d/qos.conf

Se insertan los siguienes comandos en el archivo creado:

1. ## QoS Configuracion
2. <IfModule mod_qos.c>
3. #Manejo de conexiones hasta 100000 IPs diferentes
4. QS_ClientEntries 100000
5. # Se permite solamente 50 connexiones por IP
6. QS_SrvMaxConnPerIP 50
7. # Maximo numero de conexiones TCP activas 256
8. MaxClients 256

9. # Desactivar la directiva keep-alive cuando el 70% de las conexiones TCP estan ocupadas:
10. QS_SrvMaxConnClose 70%
11. # Minimo de velocidad para peticiones / respuestas (niega a los clientes lentos que bloquean el servidor ,
12. #Ejemplo; el script slowloris mantiene las peticiones HTTP :
13. QS_SrvMinDataRate 150 1200
14. # Limite de peticiones de encabezados y cuerpo (con cuidado, limita las cargas y las peticiones POST):
15. # LimitRequestFields 30
16. # QS_LimitRequestBody 102400
17. </IfModule>

Se teclea control + x para salir y :wq para salir del archivo guardando.

Se reinicia el servicio httpd:

service httpd restart

**ANEXO O:** TIEMPOS DE LOS ATAQUES INSTALADO MOD_QOS.

| | **MEDICINA** | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en cargar por primera vez)** | **Metasploit(Tiempo se demora en cargar por primera vez)** |
| 649207734 | 27.32 | 13.16 |
| 749684523 | 38.35 | 14.03 |
| 694793613 | 34.18 | 12.53 |
| 734297481 | 27.67 | 12.15 |
| 773498541 | 39.14 | 12.51 |
| 742097705 | 19.8 | 11.98 |
| 750945494 | 27.23 | 13.89 |
| 838064475 | 27.11 | 13.23 |
| 631401534 | 26.95 | 12.77 |
| 1374642056 | 25.97 | 14.11 |
| 1000654319 | 26.75 | 13.94 |
| 787606614 | 26.34 | 13.57 |
| 877280028 | 39.87 | 13.22 |
| 676079237 | 22.74 | 12.48 |
| 135966421 | 31.55 | 11.64 |
| 716205127 | 25.28 | 13.33 |
| 444123232 | 27.18 | 12.87 |
| 496610887 | 26.93 | 11.94 |
| 1276613488 | 38.83 | 13.78 |
| 635590275 | 34.41 | 12.14 |
| 1218596770 | 27.93 | 13.23 |
| | 26.56 | 13.95 |
| 669847042 | 19.92 | 12.29 |
| 1185732117 | 39.05 | 13.86 |
| 651908738 | 21.51 | 13.15 |
| 641683132 | 30.22 | 12.03 |
| 686294023 | 31.42 | 13.11 |
| 580804867 | 27.1 | 12.36 |
| 1122656857 | 32.62 | 13.87 |
| 452206640 | 26.09 | 12.56 |

| | MEDICINA | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en cargar despues del ataque)** | **Metasploit(Tiempo se demora en cargar despues del ataque)** |
| 649207734 | 25.53 | 12.98 |
| 749684523 | 17.76 | 13.12 |
| 694793613 | 16.86 | 12.01 |
| 734297481 | 29.13 | 11.56 |
| 773498541 | 29.16 | 11.87 |
| 742097705 | 18.88 | 12.56 |
| 750945494 | 26.03 | 12.41 |
| 838064475 | 18.35 | 12.63 |
| 631401534 | 25.37 | 12.08 |
| 1374642056 | 18.19 | 13.01 |
| 1000654319 | 18.79 | 12.23 |
| 787606614 | 26.02 | 12.88 |
| 877280028 | 29.71 | 12.14 |
| 676079237 | 18.4 | 11.98 |
| 135966421 | 26.87 | 12.05 |
| 716205127 | 17.53 | 13.01 |
| 444123232 | 17.57 | 12.51 |
| 496610887 | 25.1 | 12.49 |
| 1276613488 | 29.11 | 13 |
| 635590275 | 27 | 12.94 |
| 1218596770 | 17.09 | 12.45 |
| | 26.05 | 12.56 |
| 669847042 | 19.85 | 11.93 |
| 1185732117 | 17.94 | 12.96 |
| 651908738 | 18.15 | 12.81 |
| 641683132 | 17.61 | 11.2 |
| 686294023 | 23.26 | 12.01 |
| 580804867 | 24.86 | 11.65 |
| 1122656857 | 28.92 | 12.14 |
| 452206640 | 20.7 | 11.98 |

| | DTIC | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en cargar por primera vez)** | **Metasploit(Tiempo se demora en cargar por primera vez)** |
| 649207734 | 28.51 | 13.33 |
| 749684523 | 26.43 | 13.45 |
| 694793613 | 27.65 | 11.91 |
| 734297481 | 20.45 | 11.8 |
| 773498541 | 33.98 | 12.65 |
| 742097705 | 19.16 | 12.35 |
| 750945494 | 27.12 | 13.23 |
| 838064475 | 27.81 | 13.54 |
| 631401534 | 13.37 | 11.98 |
| 1374642056 | 37.31 | 14.98 |
| 1000654319 | 39.83 | 14.01 |
| 787606614 | 26.52 | 13.21 |
| 877280028 | 15.53 | 13.94 |
| 676079237 | 27.77 | 12.01 |
| 135966421 | 33.25 | 11.03 |
| 716205127 | 29.06 | 13.38 |
| 444123232 | 15.53 | 11.24 |
| 496610887 | 21.97 | 11.69 |
| 1276613488 | 26.27 | 14.89 |
| 635590275 | 26.68 | 12.74 |
| 1218596770 | 30.03 | 14.03 |
| | 38.23 | 14.64 |
| 669847042 | 38.81 | 12.08 |
| 1185732117 | 35.08 | 14.01 |
| 651908738 | 28.04 | 13.02 |
| 641683132 | 35.55 | 12.46 |
| 686294023 | 38.78 | 12.96 |
| 580804867 | 34.95 | 11.98 |
| 1122656857 | 36.47 | 15.03 |
| 452206640 | 28.1 | 11.69 |

| | DTIC | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en cargar despues del ataque)** | **Metasploit(Tiempo se demora en cargar despues del ataque)** |
| 649207734 | 13.21 | 14.17 |
| 749684523 | 15.54 | 14.08 |
| 694793613 | 14.12 | 13.01 |
| 734297481 | 30.09 | 13.54 |
| 773498541 | 28.97 | 12.25 |
| 742097705 | 19.06 | 13.01 |
| 750945494 | 13.21 | 12.56 |
| 838064475 | 13.43 | 12.97 |
| 631401534 | 13.99 | 11.06 |
| 1374642056 | 14.06 | 13.58 |
| 1000654319 | 21.04 | 13.76 |
| 787606614 | 19.37 | 12.45 |
| 877280028 | 14.12 | 13.52 |
| 676079237 | 20.21 | 12.98 |
| 135966421 | 20.07 | 12.47 |
| 716205127 | 26 | 13.23 |
| 444123232 | 14.21 | 12.02 |
| 496610887 | 19.22 | 12.15 |
| 1276613488 | 23.11 | 13.96 |
| 635590275 | 20.26 | 13.01 |
| 1218596770 | 19.87 | 13.98 |
| | 22.33 | 14.02 |
| 669847042 | 21.09 | 12.87 |
| 1185732117 | 21.83 | 13.54 |
| 651908738 | 19.66 | 13.43 |
| 641683132 | 19.07 | 13.21 |
| 686294023 | 27.92 | 13.74 |
| 580804867 | 19.11 | 13.01 |
| 1122656857 | 20.01 | 14.09 |
| 452206640 | 19.58 | 12.86 |

| | SISTEMA WEB ACADÉMICO | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en cargar por primera vez)** | **Metasploit(Tiempo se demora en cargar por primera vez)** |
| 649207734 | 29.09 | 13.52 |
| 749684523 | 21.04 | 13.02 |
| 694793613 | 31.74 | 12.49 |
| 734297481 | 25.89 | 13.38 |
| 773498541 | 32.45 | 12.98 |
| 742097705 | 21.54 | 12.36 |
| 750945494 | 28.11 | 13.01 |
| 838064475 | 26.54 | 13.27 |
| 631401534 | 22.88 | 12.61 |
| 1374642056 | 31.36 | 14.78 |
| 1000654319 | 32.73 | 13.87 |
| 787606614 | 26.98 | 13.31 |
| 877280028 | 25.31 | 13.69 |
| 676079237 | 23.15 | 13.08 |
| 135966421 | 30.54 | 12.54 |
| 716205127 | 27.01 | 12.98 |
| 444123232 | 23.69 | 11.78 |
| 496610887 | 25.87 | 12.32 |
| 1276613488 | 30.09 | 12.74 |
| 635590275 | 31.32 | 13.27 |
| 1218596770 | 26.98 | 13.96 |
| | 33.74 | 14.87 |
| 669847042 | 30.53 | 13.96 |
| 1185732117 | 36.02 | 14.74 |
| 651908738 | 27.63 | 13.71 |
| 641683132 | 31.25 | 13.09 |
| 686294023 | 33.74 | 14.03 |
| 580804867 | 30.54 | 12.78 |
| 1122656857 | 30.87 | 13.27 |
| 452206640 | 27.93 | 12.35 |

| | SISTEMA WEB ACADÉMICO | |
|---|---|---|
| **Paquetes** | **Slowloris(Tiempo se demora en cargar despues del ataque)** | **Metasploit(Tiempo se demora en cargar despues del ataque)** |
| 649207734 | 19.36 | 16.51 |
| 749684523 | 15.91 | 12.45 |
| 694793613 | 20.11 | 12.01 |
| 734297481 | 24.1 | 13.74 |
| 773498541 | 27.45 | 12.05 |
| 742097705 | 17.54 | 12.96 |
| 750945494 | 19.63 | 13.54 |
| 838064475 | 17.98 | 13.01 |
| 631401534 | 21.24 | 13.88 |
| 1374642056 | 19.67 | 13.5 |
| 1000654319 | 20.87 | 12.43 |
| 787606614 | 25.02 | 12.74 |
| 877280028 | 23.15 | 12.96 |
| 676079237 | 19.49 | 12.35 |
| 135966421 | 22.14 | 11.41 |
| 716205127 | 19.73 | 11.87 |
| 444123232 | 20.08 | 12.54 |
| 496610887 | 22.95 | 12.35 |
| 1276613488 | 21.5 | 12.01 |
| 635590275 | 23.63 | 12.87 |
| 1218596770 | 20.07 | 13.02 |
| | 19.39 | 13.13 |
| 669847042 | 19.46 | 12.86 |
| 1185732117 | 20.89 | 13.45 |
| 651908738 | 19.08 | 12.87 |
| 641683132 | 18.98 | 11.39 |
| 686294023 | 24.13 | 13.24 |
| 580804867 | 20.96 | 12.99 |
| 1122656857 | 23.57 | 12.1 |
| 452206640 | 20.81 | 11.08 |

**ESCUELA SUPERIOR POLITÉCNICA DE**

**CHIMBORAZO**

**DIRECCIÓN DE BIBLIOTECAS Y RECURSOS**

**PARA EL APRENDIZAJE Y LA INVESTIGACIÓN**

**UNIDAD DE PROCESOS TÉCNICOS**

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN YBIBLIOGRAFÍA

**Fecha de entrega:**

| **INFORMACIÓN DEL AUTOR/A (S)** |
|---|
| **Nombres – Apellidos:** |
| **INFORMACIÓN INSTITUCIONAL** |
| **Facultad:** |
| **Carrera:** |
| **Título a optar:** |
| **f. Analista de Biblioteca responsable:** |