UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CARRERA DE SISTEMAS Y COMPUTACIÓN

Proyecto de Investigación previo a la obtención del título de Ingeniero en Sistemas y Computación

DETECCIÓN Y EVALUACIÓN DE VULNERABILIDADES EN LA WEB CON LA TÉCNICA BANNER GRABBING EN LA COOPERATIVA DE AHORRO Y CRÉDITO "RIOBAMBA" LTDA.

AUTOR:

Francisco Manuel Pérez Rosero

TUTOR:

Ing. Lorena Paulina Molina Valdiviezo., Ph. D.

RIOBAMBA - ECUADOR

2020

VEREDICTO DE LA INVESTIGACIÓN

Los miembros del Tribunal de Graduación del proyecto de investigación de título: **"Detección y Evaluación de Vulnerabilidades en la Web con la Técnica Banner Grabbing en la Cooperativa de Ahorro y Crédito "Riobamba" Ltda."**, presentado por el Sr. Francisco Manuel Pérez Rosero y dirigida por: PhD. Lorena Molina Valdiviezo.

Una vez escuchada la defensa oral y revisando el informe final del proyecto de investigación con fines de graduación escrito en el cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

PhD. Lorena Molina ……

Director del Proyecto Firma

Ing. Luis Tello ……

Miembro del Tribunal Firma

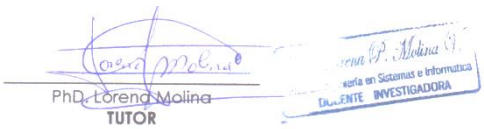
Ing. Diego Reina ……

Miembro del Tribunal Firma

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad del contenido de este Proyecto de Graduación corresponde exclusivamente al Sr. Francisco Manuel Pérez Rosero, autor del proyecto de investigación y PhD. Lorena Paulina Molina Valdiviezo tutora de tesis; el patrimonio intelectual de la misma a la Universidad Nacional de Chimborazo.

Francisco Manuel
Pérez Rosero
C.I. 060411154-2



Ing. Lorena Paulina
Molina Valdiviezo PhD
C.I. 060322815-6

DEDICATORIA

Dedico este proyecto de investigación en primer lugar a mis padres por brindarme su apoyo y confianza en todo momento, a mis hermanos que siempre han estado pendientes de mí, apoyándome y guiándome con sus consejos a pesar de la distancia, a mi esposa Gaby y a mi hija Gaia que son el motor para seguir adelante y fuerza para ser cada día mejor, a mis amigos con los cuales compartí grandes momentos en las aulas de la universidad y que estoy seguro que la amistad perdurará por muchos años más y, por último, pero no menos importante a todas las personas que de una u otra manera contribuyeron a que esta meta se cumpla.

Francisco Manuel Pérez Rosero

AGRADECIMIENTO

En la presente investigación quiero agradecer en primer lugar a mis padres por ser un pilar fundamental en este logro y su apoyo incondicional en esta etapa de mi vida.

A la Universidad Nacional de Chimborazo que se convirtió en mi segundo hogar, a mis docentes que me compartieron sus conocimientos, no solo académicos sino también personales como consejos para la vida.

Agradezco de manera muy especial a la Ing. Lorena Molina Valdiviezo, Ing. Luis Tello e Ing. Diego Reina tutores de mi proyecto de investigación por guiarme con sabiduría, rectitud y paciencia para poder culminar esta meta académica de manera satisfactoria.

Francisco Manuel Pérez Rosero

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Hoy en día la información se ha convertido en un bien sumamente importante y con ello surge la necesidad de protegerla de los ataques que pueden afectar su integridad o su confidencialidad. Esta necesidad es más preponderante si dicha información se trata de una entidad bancaría como lo es la Cooperativa de ahorro y Crédito "Riobamba" Ltda. ya que maneja información personal, de cuentas bancarias e inversiones de sus socios, haciendo que estos datos sean un blanco muy apetecido para delincuentes informáticos.

La metodología utilizada en la investigación es inferencial por el análisis pre y post acerca de las vulnerabilidades y riesgos. Además, se muestran en el estudio tres escenarios: el primero simulando la topología de red de la cooperativa con una concurrencia típica y sin ningún tipo de ataque informático; el segundo aplicando ataques informáticos usando para ello la técnica banner grabbing al escenario anteriormente mencionado con el fin de analizar qué tan vulnerable es la topología de red; y en el tercer escenario se implementan mecanismos de defensa, para medir como repercuten en la seguridad informática.

Se realizó escaneos de puertos abiertos/cerrados; además, se midieron tiempos de respuesta del servidor web obteniendo una mejora de 14.8 milisegundos, el uso del CPU se redujo al 37% y el consumo de memoria RAM se minimiza al 39%. Tras aplicar el firewall FortiWeb confirmando así la efectividad de la implementación de los mecanismos de defensa.

Palabras claves: Ataques Informáticos, Banner Grabbing, Ciberseguridad, Simulación.

ABSTRACT

Today, information has become an extremely important asset and with this increased need to protect it from attacks that may affect its integrity or confidentiality. This need is more important if this information is about a banking entity such as the "Riobamba" Ltda. Savings and Credit Cooperative, since it manages personal information, bank accounts and investments of its members, making these data a target Very tempting for cybercriminals. The methodology used in the investigation is inferential for pre and post analysis of vulnerabilities and risks. In addition, three scenarios are shown in the study: the first simulating the cooperative's network topology with a typical concurrence and without any type of computer attack; the second applying computer attacks using the banner grabbing technique to the aforementioned scenario in order to analyze how vulnerable the network topology is; and in the third scenario, defense mechanisms are implemented to measure how are the repercussions on computer security. Open / closed port scans were performed; In addition, response times of the web server were measured, obtaining an improvement of 14.8 milliseconds, CPU usage was reduced to 37% and RAM consumption was minimized to 39%. After applying the FortiWeb firewall, confirming the effectiveness of the implementation of defense mechanisms.

Keywords: Computer Attacks, Banner Grabbing, Cybersecurity, Simulation.

Reviewed by:
Danilo Yépez Oviedo
English professor UNACH

INTRODUCCIÓN

Debido a la globalización, la información ha tomado un papel muy importante en cualquier organización. Además, debido al avance tecnológico, todas las organizaciones se han visto en la necesidad de adaptarse y sistematizar su información. Es por esto que en todo el mundo ocurren diferentes tipos de ataques informáticos a diario, lo que puede llevar a daños y alteraciones en la información. Esto conlleva a un gran problema ya que actualmente la información se ha convertido en uno de los activos más importantes de las organizaciones y al verse afectada puede causar daños económicos irreparables (Vvasquez, 2018).

Por otra parte, el impacto y costo del cibercrimen siguen en aumento. Un informe realizado por Cybersecurity Ventures en 2017 (Herjavec Group, 2017) señala que en 2021 habrá 3.5 millones de nuevos puestos de trabajo en ciberseguridad. Sin embargo, las previsiones de empleos en seguridad cibernética no han podido seguir el ritmo del espectacular aumento del cibercrimen, ya que se provee que este le costará al mundo 6 mil millones de dólares (mdd) anuales.

La detección y evaluación de las vulnerabilidades en la web usando la técnica Banner Grabbing ayudó a mejorar la seguridad informática de la red de la Cooperativa de Ahorro y Crédito (COAC) “Riobamba” Ltda., al conocer cuáles son sus falencias en cuanto a puertos abiertos y ataques más comunes a su servidor web; con ello se aplicaron medidas de seguridad como la implementación de un firewall especializado que ayuda a filtrar de mejor manera posibles ataques desde internet. Adicionalmente, para comprobar la eficacia de este firewall, se implementó un escenario simulado con la misma topología de red usada dentro de la COAC “Riobamba” Ltda.

CAPÍTULO I

Planteamiento del problema

Problema y Justificación

En la actualidad, las nuevas tecnologías están al alcance de nuestras manos. Dedicamos gran parte de nuestro tiempo a un mundo computarizado, en forma de datos los cuales pueden ser sustraídos y manipulados para el beneficio ajeno. Es por ello que las redes y sistemas informáticos deben estar protegidos y asegurados ante la amenaza del robo de la privacidad de los datos. El tema se acentúa cuando incorporamos información sensible de las empresas cuyo valor puede ser incalculable y puede determinar el éxito o fracaso.

El sector financiero se encuentra entre los sectores económicos más avanzados en lo que respecta al uso de Tecnologías de la Información (TI) y, lógicamente, ha invertido muchos recursos en dichos sistemas de seguridad. Además, es una de las industrias más interconectadas, y un objetivo claro para los ciberdelincuentes. La amenaza y el impacto de los ataques en la industria están en aumento, y el sector está buscando cada vez más formas de enfrentar el riesgo cibernético y la ciberseguridad (Organización de los Estados Americanos, 2018).

Según estudios realizados por expertos de seguridad informática, el 92% de las entidades bancarias manifiestan que identificaron algún tipo de evento (ataques exitosos y ataques no exitosos) en contra de la entidad financiera. Los eventos más identificados fueron: i) el código malicioso o malware (80% del total de entidades bancarias), ii) la violación de políticas de escritorio limpio (clean desk) (63% del total de entidades bancarias), y, iii) el phishing dirigido para tener acceso a sistemas del banco (57% del total de entidades bancarias). Además, las entidades financieras detectaron eventos con frecuencia diaria de malware y phishing (un 24% y 22%, respectivamente) dirigidos para tener acceso a los sistemas del banco. Respecto a la

gestión, respuesta y recuperación ante incidentes de seguridad digital, al menos la mitad de las entidades bancarias de la región contaron con estrategias de gestión, respuesta y recuperación ante incidentes de seguridad digital (Organización de los Estados Americanos, 2018).

Es por esto que la red de la COAC "Riobamba" Ltda. no es la excepción; según el departamento de tecnologías de la información ésta ha sufrido diversos ataques informáticos poniendo en riesgo los servicios que ofrece y a sus socios.

Con los resultados del proyecto de investigación "DETECCIÓN Y EVALUACIÓN DE VULNERABILIDADES EN LA WEB CON LA TÉCNICA BANNER GRABBING EN LA COOPERATIVA DE AHORRO Y CRÉDITO "RIOBAMBA" LTDA. se podrá prever ataques informáticos dentro de su infraestructura web y evaluar las vulnerabilidades existentes obteniendo de esta manera un manual para conocer, actuar y prevenir este tipo de ataques.

Banner Grabbing es una técnica que permite obtener información del servidor web, hasta llegar a mostrar la versión del servidor de esta manera sustraer datos sensibles (SniferLabs, 2016).

Objetivos

Objetivo General

- Detectar y evaluar las vulnerabilidades en la web utilizando la técnica Banner Grabbing en la COAC “Riobamba” Ltda.

Objetivos Específicos

- Analizar las vulnerabilidades existentes en la web.
- Estudiar la técnica Banner Grabbing para la detección de vulnerabilidades.
- Identificar y evaluar las vulnerabilidades de la COAC “Riobamba” Ltda.
- Elaborar un manual para mejorar la seguridad en la web de la COAC “Riobamba” Ltda.

CAPITULO II

2. Marco Teórico

2.1 Seguridad Informática

Podemos definir como seguridad informática al proceso de establecer y observar un conjunto de estrategias, políticas y procedimientos para prevenir daño, alteración o sustracción los recursos informáticos de una organización además de garantizar el correcto funcionamiento de esos recursos. (Silvia M. Quiroz-Zambrano, 2017).

2.2 Seguridad de la información

Para ISOTools Excellence (2017), la definición de la seguridad de la información tributa a una disciplina que se encarga de la implementación técnica de la protección de la información; es decir, el despliegue de las tecnologías que establecen de qué forma que se aseguran las situaciones de fallas y más aún cuando la información es el activo que se encuentra en riesgo (ISOTools Excellence, 2017).

2.3 Amenazas Informáticas

Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientas, hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información.

En función del tipo de alteración, daño o intervención que podrían producir sobre la información, las amenazas se clasifican en cuatro grupos:

Tabla 1: Tipos de ataques informáticos

Tipo de ataque	Descripción
De interrupción	El objetivo de las amenazas es deshabilitar el acceso a la información.
De interceptación	Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización.
De modificación	Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización.
De fabricación	Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización.

En sistemas de información como los que manejan las instituciones financieras la presencia de amenazas informáticas es un factor muy importante a tomar en cuenta por lo cual se debe identificar las alteraciones que estos sistemas podrían sufrir (López, 2016).

2.4 Riesgos informáticos

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe una amenaza para la misma (López, 2016).

Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

1. Asumirlo sin hacer nada. Esto resulta lógico cuando el prejuicio esperando no tiene valor alguno o cuando el coste de aplicación de medidas superaría a la del valor de daño.
2. Aplicar medidas para disminuirlo o anularlo.
3. Transferirlo (por ejemplo, contratando un seguro).

2.5 Ataques en la red

Se dice que se ha producido un ataque accidental o deliberado contra el sistema cuando se ha materializado una amenaza.

En función del tipo de impacto causado a los activos atacados, los ataques se clasifican en:

- **Activos.** Si se modifican, dañan, suprimen o agregan información, o bien bloquean o saturan los canales de comunicación.
- **Pasivos.** Solamente acceden sin autorización a los datos contenidos en el sistema. Son los más difíciles de detectar.

Un ataque puede ser directo o indirecto, si se produce desde el atacante al elemento o victima directamente, o a través de recursos o personas intermediarias (López, 2016).

2.5.1 Análisis de tráfico

Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los "sniffers". Así, se conoce como "eavesdropping" a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido. Una organización podría protegerse frente a los "sniffers" recurriendo a la utilización de redes conmutadas ("switches" en lugar de "hubs") y de redes virtuales de área local (VLAN).

No obstante, en redes locales que utilizan "switches" (es decir, en redes conmutadas), un atacante podría llevar a cabo un ataque conocido como "MAC flooding" para provocar un

desbordamiento de las tablas de memoria de un switch (tablas denominadas CAM por los fabricantes, “Content Addresable Memory”) para conseguir que pase a funcionar como un simple “hub” y retransmita todo el tráfico que recibe a través de sus puertos (al no poder “recordar” qué equipos se encuentran conectados a sus distintas bocas o puertos por haber sido borradas sus tablas de memoria) (Vieites, TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS, 2016).

2.5.2 DNS Spoofing

Los ataques de falsificación de DNS pretenden provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas Web falsas o bien la interceptación de sus mensajes de correo electrónico. Para ello, en este tipo de ataque los intrusos consiguen que un servidor DNS legítimo acepte y utilice información incorrecta obtenida de un ordenador que no posee autoridad para ofrecerla. De este modo, se persigue “inyectar” información falsa en el base de datos del servidor de nombres, procedimiento conocido como “envenenamiento de la caché del servidor DNS”, ocasionando con ello serios problemas de seguridad (Vieites, TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS, 2016).

2.5.3 IP Spoofing

Los ataques de suplantación de la identidad presentan varias posibilidades, siendo una de las más conocidas la denominada “IP Spoofing” (“enmascaramiento de la dirección IP”), mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado. Así, por ejemplo, el atacante trataría de seleccionar una dirección IP

correspondiente a la de un equipo legítimamente autorizado para acceder al sistema que pretende ser engañado. Los propietarios de las redes y operadores de telecomunicaciones podrían evitar en gran medida el "IP Spoofing" implantando filtros para que todo el tráfico saliente de sus redes llevara asociado una dirección IP de la propia red desde la que se origina el tráfico (Cordero, 2016).

2.5.4 Ataques de Inyección de Código SQL

"Structured Query Language" (Lenguaje de Consulta Estructurado) (SQL), es un lenguaje textual utilizado para interactuar con bases de datos relacionales. La unidad típica de ejecución de SQL es la consulta ("query"), conjunto de instrucciones que permiten modificar la estructura de la base de datos (mediante instrucciones del tipo "Data Definition Language", DDL) o manipular el contenido de la base de datos (mediante instrucciones del tipo "Data Manipulation Language", MDL). En los servidores Web se utiliza este lenguaje para acceder a bases de datos y ofrecer páginas dinámicas o nuevas funcionalidades a sus usuarios. El ataque por inyección de código SQL se produce cuando no se filtra de forma adecuada la información enviada por el usuario. Un usuario malicioso podría incluir y ejecutar textos que representen nuevas sentencias SQL que el servidor no debería aceptar. Este tipo de ataque es independiente del sistema de bases de datos subyacente, ya que depende únicamente de una inadecuada validación de los datos de entrada. Como consecuencia de estos ataques y, dependiendo de los privilegios del usuario de base de datos bajo el cual se ejecutan las consultas, se podría acceder no sólo a las tablas relacionadas con la operación de la aplicación del servidor Web, sino también a las tablas de otras bases de datos alojadas en el mismo servidor Web. También pueden propiciar la ejecución de comandos arbitrarios del sistema operativo del equipo del servidor Web (Racciatti, 2016).

2.5.5 Denegación del Servicio (Ataques DoS – Denial of Service)

Los ataques de Denegación de Servicio (DoS) consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes informáticos, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios. Para ello, existen varias posibilidades de conseguirlo:

- Ejecutar algunas actividades que produzcan un elevado consumo de los recursos de las máquinas afectadas: procesador, memoria y/o disco duro, provocando una caída en su rendimiento. Entre ellas podríamos citar el establecimiento de múltiples conexiones simultáneas, el envío masivo de ficheros de gran tamaño o los ataques lanzados contra los puertos de configuración de los routers.
- Provocar el colapso de redes de ordenadores mediante la generación de grandes cantidades de tráfico, generalmente desde múltiples equipos.
- Transmisión de paquetes de datos malformados o que incumplan las reglas de un protocolo, para provocar la caída de un equipo que no se encuentre preparado para recibir este tipo de tráfico malintencionado.

Hay que tener en cuenta que en los ataques DoS el atacante suele ocultar su verdadera dirección mediante técnicas de "IP Spoofing". Además, en numerosas ocasiones se han empleado este tipo de ataques para encubrir otros ataques simultáneos que pretendían comprometer un sistema o red informático (Bezzi, 2016).

2.6 Clasificación de los intrusos en las redes

2.6.1 Hackers

Los hackers son intrusos que se dedican a burlar sistemas de seguridad informática como pasatiempo y como reto técnico: entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos de los entresijos de Internet, pero no pretenden provocar daños en estos sistemas. Sin embargo, hay que tener en cuenta que pueden tener acceso a

información confidencial, por lo que su actividad está siendo considerada como un delito en bastantes países de nuestro entorno (Vieites, TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS, 2014).

Podemos considerar a un hacker como una persona que busca la manera de encontrar vulnerabilidades en un sistema, pero no para aprovecharse de ellas sino para intentar corregir esos errores en una red o sistema y de esa manera hacerlo más seguro.

2.6.2 Crackers

Los crackers son individuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o, simplemente, para provocar algún daño a la organización propietaria del sistema, motivada por intereses económicos, políticos, religiosos, entre otros (Vieites, TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS, 2014) .

2.7 Vulnerabilidades existentes aplicaciones web y webservers

La exposición de los servidores web y aplicaciones web a internet hacen que estos sean muy vulnerables en diferentes flancos es por ello que es muy importante analizar las vulnerabilidades que puedan existir, así como las contramedidas necesarias a tomar para que la integridad de la información no se vea afectada por un ataque informático.

2.7.1 Aplicaciones web

Estas aplicaciones son interfaces que se encuentran entre los usuarios y los webservers, usan una arquitectura cliente/servidor usando códigos JavaScript en la máquina del usuario y gestionando consultas en el servidor web. Por lo tanto, son susceptibles a ataques de manipulación de código y acciones, como inyecciones SQL explotación de vulnerabilidades XSS, hijacking, Spoofing, MITM, entre otros. Además, a partir de la llegada de la nombrada

como web 2.0, estos riesgos se han ampliado considerablemente, dado que el objetivo es crear más interactividad y movimiento a las webs tradicionales estáticas (Jiménez, 2016).

2.7.2 Vulnerabilidades en las aplicaciones web

Debido a la arquitectura general de una aplicación web, no hace falta mucho para darse cuenta de que los frentes abiertos para encontrar vulnerabilidades que explotar son numerosos. Por cada capa existirán algunos concretos y otros ámbitos más globales, pero todos aspectos importantes a tomar en cuenta.

Estos aspectos se pueden enumerar de la siguiente manera:

1. **Manipulación de parámetros:** en ocasiones es posible manipular los parámetros de entrada (por ejemplo, al conectarse con un webserver) con el fin de modificar permisos de sesión, editar variables, etc. Por ejemplo, en una URL puede aparecer algún parámetro que sea susceptible de modificar manualmente su valor para acceder a un sitio o modificar algún campo.
2. **Directorios transversales:** podemos encontrar vulnerabilidades asociadas a la mala configuración de los accesos a los directorios. Por ejemplo, en una URL vulnerable, un atacante puede introducir manualmente código como .../ y acceder a algunos directorios *root* o a algunos que no debería tener acceso. También explorando los paquetes de intercomunicación, se puede introducir código malicioso explotando esta vulnerabilidad. (Vieites, TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS, 2016).
3. **Inyecciones de código:** consiste en inyectar códigos, comandos o archivos con un determinado formato en las consultas de una web (consultas a su base de datos) o en las comunicaciones de las API's para aprovecharse de una vulnerabilidad concreta conocida. Existen tres tipos de inyecciones; SQL el cual se hablará con detalle en punto

9.3, Inyección de comandos, los cuales manipulan los códigos de HTML, PHP o Shell para ganar acceso al servidor o infectarlo con malware subiendo archivos.

4. **XSS (Cross-Site Scripting):** Consiste explotar vulnerabilidades de webs consideradas 2.0 con el objetivo de inyectar un script malicioso para que los demás usuarios lo visualicen. Esto ocurre porque muchas de estas webs son generadas dinámicamente. Por ejemplo, inyectando un script en PHP dentro del marco HTML, se genera una respuesta errónea al resto de usuarios de esa misma aplicación web, por ejemplo, redirigiéndolos a un servidor infectado.

2.7.3 Herramientas para explotar vulnerabilidades en aplicaciones web

Algunas de las herramientas más utilizadas para explotar vulnerabilidades de aplicaciones web pueden ser:

- **Explotación de aplicaciones web:** Burp Suite Professional, CookieDigger, WebScarab, Instant SOurce, WebCopier, HHTtrack, HttpBee, W3af o BlackWidow.
- **Seguridad en aplicaciones web:** tenemos algunas como Acunetix Web Vulnerability Scanner, Watcher Web Security Tool, Netparker, N-Stalker, Web Application Security Scanner, VampireScan, OWASP ZAP, NetBrute, Syhunt Mini, SPIKE proxy o WSSA Web site Security Audit, entre otras.
- **Firewalls a nivel de aplicación web:** dotDefender, ServerDefender VP, Radware's AppWall, Barracuda Web Application Firewall, ThreatSentry, IBM Security AppScan o ModSecurity, entre otros.

2.8 Webservers

En el ámbito de los servidores, hay que aclarar varios conceptos de seguridad importantes dado que son susceptibles de muchos ataques. Son equipos conectados a Internet, que soportan

muchas aplicaciones web y software, además de alojar bases de datos, webs, servicios, entre otros. Así que son objetivos expuestos que hay que proteger. Procesos como el hardening se ocupan de fortalecer estos webservers ante todo tipo de ataques.

Los impactos de los ataques que comprometen a los servidores suelen ser muy graves dado que se extrapolan a muchos otros campos; redes, servicios, maquinas conectadas, bases de datos sensibles. Los objetivos más comunes suelen ser comprometer la información de los usuarios pivotar para acceder a los servicios web (Muñoz, 2018).

Normalmente la arquitectura de un webserver suele ser la de un sistema junto a un sistema operativo especialmente diseñado para las tareas de servir/recibir (por ejemplo, Windows server o Apache). Estos sistemas suelen ser escalables y ejecutan tareas web basadas en lenguajes de programación destinados a tal fin como PHP, bases de datos y por supuesto alojan los archivos físicamente. A su vez necesitan un cliente, un programa que sea capaz de comunicarse con él, pude ser un navegador web, o un programa especial. A través de esto, los usuarios comunes realizan las tareas. Además, el administrador suele tener permisos especiales para poder gestionar y analizar el contenido del servidor, ya puede ser remota o localmente. Dado que estas conexiones se realizan a través de Internet normalmente, los atacantes aprovechan este flanco para encontrar vulnerabilidades y explotarlas (Vieites, TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS, 2016).

Como es lógico existen una gran variedad de posibles ataques y técnicas de explotación que se explicarán a continuación.

- **DNS hacking:** mediante consultas incorrectas y/o falsas, procedente de un boot por decir un ejemplo, se puede provocar la caída de los servidores.
- **Recursive DNS:** este ataque es derivado del anterior, y consiste en comprometer los servidores DNS para que haga más consultas de las habituales a sus servidores DNS

vecinos en busca de un dominio concreto. Esto puede usarse para amplificar los ataques a diversos servidores DNS.

- **Directorios transversales:** de igual manera que con las aplicaciones web, existe la posibilidad que un atacante pueda acceder a un directorio que no debería introduciendo rutas ambiguas como …/. Este error de configuración suele ser bastante común.
- **Phishing:** Este tipo de ataque son un gran frente de ataques constantes hacia los usuarios incluso administradores de los servidores. El objetivo de este tipo de ataque siempre será robar las credenciales a los usuarios legítimos a servidores comprometidos, o infectar sus máquinas.
- **Defectos de configuración:** existen defectos de configuraciones susceptibles de ser debilidades. Passwords y users por defecto, mensajes de error que dan demasiada información, certificados SSL y configurados por defecto, servicios y puertos activos innecesarios, posibilidades de introducir scripts en las consultas, descontrol de las consultas, así como url no normalizadas, entre otros.
- **Ataque SSH por fuerza bruta**: como su nombre indica, consiste en aplicar ataques de fuerza bruta a los logins del protocolo SSH utilizado por los administradores para obtener acceso no autorizado con privilegios.
- **Ataques a contraseñas:** los ataques a contraseñas, son objeto de black hats. Normalmente los objetivos suelen ser protocolos SMTP, SSH, FTP. mediante uso de ingeniería social, Phishing, Spoofing, entre otros.

2.9 Técnica Banner Grabbing

Uno de los aspectos a la hora de realizar controles sobre una aplicación web es la información que puede obtenerse a través de lo que se conoce como banner grabbing. Este concepto se refiere a la interacción manual en texto plano para obtener información sobre sobre el servidor

donde reside la aplicación web. Si bien la técnica de banner grabbing puede aplicarse sobre cualquier tipo de servicio, cómo, por ejemplo, FTP, VNC, HTTP, entre otros, en este caso nos enfocaremos sobre el último debido a que es posible resaltar comportamientos particulares del mismo. Además de la detección del servidor que se aloja detrás del sitio web, en algunos casos es posible conocer la versión del mismo. Cabe destacar que no siempre es posible obtener información completa ya que existen formas de ocultar la información que brinda un servidor frente a diferentes peticiones (Catoira, 2017).

2.9.1 Herramientas para Banner Grabbing

Las herramientas comúnmente utilizadas para realizar el Banner Grabbing son Telnet, Nmap y Netcat. Aunque podemos incluir otras que tienen ciertas funcionalidades las cuales nos permiten analizar vulnerabilidades, a continuación, veremos más a detalle cuales son estas herramientas:

2.9.2 Netcat

Netcat es una herramienta de red que permite a través de intérprete de comandos y con una sintaxis sencilla abrir puertos TCP/UDP en un HOST (quedando Netcat a la escucha), asociar una Shell a un puerto en concreto (para conectarse por ejemplo a MS-DOS o al intérprete bash de Linux remotamente) y forzar conexiones UDP/TCP (útil por ejemplo para realizar rastreos de puertos o realizar transferencias de archivos bit a bit entre dos equipos) (Giacobbi, 2016).

2.9.3 Nmap

Es un programa de código abierto lanzado bajo la licencia Publica General de GNU. Es una herramienta muy potente para administradores de red ya que puede ser utilizado para descubrir,

monitorear y solucionar problemas de los sistemas TCP/IP. Puede ser utilizada también como una utilidad de exploración de red multiplataforma (NMAP.ORG, 2015).

2.9.4 Zenmap

Zenmap es la interfaz gráfica de usuario de Nmap Security Scanner. Es una aplicación multiplataforma y de código abierto que tiene como objetivo hacer que Nmap sea fácil de usar para principiantes al mismo tiempo que proporciona funciones avanzadas para usuarios con experiencia en Nmap. Además, tiene funcionalidades como la de guardar los escaneos utilizados con frecuencia para ejecutarlos posteriormente (Luz, 2014).

2.10 Funcionamiento de la técnica Banner Grabbing

El banner grabbing es una de las formas de conocer qué infraestructura o sistema se encuentra detrás de una aplicación web o servicio. En otras palabras, está fuertemente relacionado con el *fingerprinting* para detectar el sistema operativo.

Si bien el método de banner grabbing puede aplicarse sobre cualquier tipo de servicio cómo, por ejemplo, FTP, VNC, HTTP, entre otros, en este estudio nos enfocaremos sobre el último debido a que es posible resaltar comportamientos particulares del mismo. Además de la detección del servidor que se aloja detrás del sitio web, en algunos casos es posible conocer la versión del mismo. A continuación, podremos ver un gráfico que resume el funcionamiento de banner grabbing:

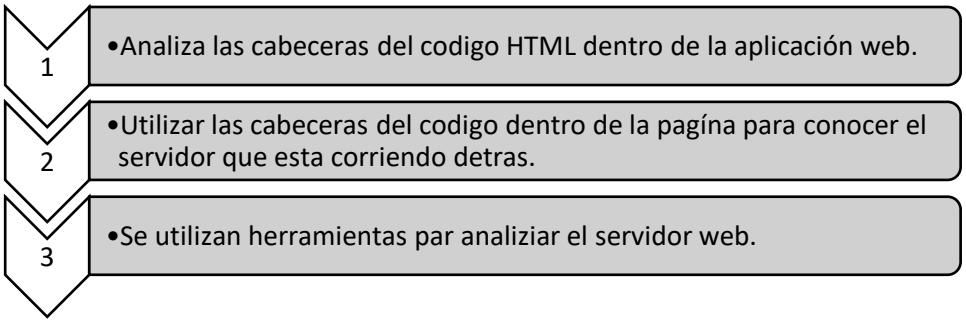


Figura 1: Funcionamiento de Banner Grabbing

CAPÍTULO III

3. Metodología

El diseño de la investigación utilizó un tipo de estudio cuantitativo ya que con dicho estudio se garantizó la medición de variables establecidas en la investigación para la detección y posterior evaluación de las vulnerabilidades en la web con la técnica Banner Grabbing.

Según el nivel de medición y análisis de la información fue una investigación descriptiva e inferencial ya que se realizó un análisis previo y post acerca de las vulnerabilidades y riesgos en la red de la COAC "Riobamba Ltda. Mediante la técnica Banner Grabbing y la utilización de herramientas de simulación y mecanismos de defensa.

Según las variables fue una investigación experimental ya que como investigadores se experimentó y se probó en varios escenarios de simulación diferentes mecanismos de defensa para proteger a la red de la COAC, además de la manipulación de variables para poder comprobar la hipótesis de la investigación.

En una etapa inicial se realizaron detecciones de fallo en la infraestructura web de la COAC "Riobamba Ltda.", utilizando varias herramientas de Kali Linux hacia el servidor web en diferentes periodos de tiempo, con el fin de conocer el nivel de seguridad que esta presenta. Posteriormente se implementó mecanismos de defensa, así como añadir un segundo firewall especializado para el servidor web.

3.1 Hipótesis

Hi= La implementación de mecanismos de defensa en un ambiente simulado permite proyectar la disminución de ataques en la web de la COAC "Riobamba Ltda.".

Ho= La implementación de un mecanismo de defensa en un ambiente simulado no permite minimizar los ataques en la web de la COAC "Riobamba Ltda.".

3.2 Identificación de variables

3.2.1 Variable dependiente

Detección y Evaluación de vulnerabilidades.

3.2.2 Variable independiente

Técnica Banner Grabbing.

3.3 Tipo de estudio

3.3.1 Según el tipo de estudio

Investigación Aplicada: Se aplica una solución al problema, mediante la aplicación de mecanismos de detección y defensa híbrido frente a ataques al servidor web.

3.3.2 Según la fuente de investigación

Investigación Bibliográfica: Recolección de la información, utilizando técnicas y estrategias para acceder a documentos como: tesis, artículos científicos, libros para la investigación.

3.3.3 Según el nivel de conocimientos

Investigación Descriptiva: Se realiza un análisis sobre las vulnerabilidades y riegos que afectan la optimización de la red, mediante la medición y evaluación de diferentes parámetros, datos, componentes del fenómeno a investigar.

3.3.4 Según las variables

Investigación Experimental: Análisis de la red de la COAC "Riobamba" Ltda., con el objetivo de comprobar la hipótesis de investigación, se estudia 2 escenarios simulados. El primer escenario atacando la red sin aplicar el mecanismo de detección y defensa y el segundo aplicado mecanismos de seguridad.

3.4 Población y Muestra

Se trata de una población infinita debido a que se obtuvo datos de diferentes mediciones de ataques IP Spoofing.

La muestra que se tomó fue en base a 3 horarios de ataques en un período de tiempo de 5 días.

3.5 Unidad de Análisis

Los ataques se llevaron a cabo durante 5 días y cada día durante 3 periodos en la mañana de **09H00-13H00**, tarde de **14H00-18H00** y noche de **19H00-22H00**. Los datos obtenidos durante los ataques fueron registrados y analizados.

3.6 Operacionalización de variables

Variable	Tipo	Definición Conceptual	Dimensión	Indicadores
Técnica Banner Grabbing	Independiente	Una técnica encargada de filtrar información sobre el servidor para detectar la versión del mismo y aprovechar sus vulnerabilidades.	Ataques activos Experimentación	- Número de ataques detectados - Tiempo de Respuesta del Servidor - Uso de CPU y RAM del servidor.
Detección y evaluación de vulnerabilidades en la web	Dependiente	El primer paso para poder garantizar la seguridad de un servidor es conocer cuáles son las vulnerabilidades existentes para poder corregirlas.	Ataques activos Experimentación	- Número de ataques detectados - Tiempo de Respuesta del Servidor - Uso de CPU y RAM del Servidor

3.7 Técnicas de análisis e interpretación de la información

Para la detección y evaluación de amenazas en la web, se realizó el estudio de mecanismo de seguridad, técnicas o herramientas las cuales logran en primer lugar detectar que vulnerabilidades existen dentro de la topología de red para posteriormente mitigarlas. Para ello se plantea las siguientes acciones:

- Realización de un estudio de la situación actual de la red de la COAC “Riobamba” Ltda.
- Detección de las vulnerabilidades existentes dentro de la red.
- Evaluación de dichas vulnerabilidades y los impactos y riesgos que representan para el funcionamiento del servidor WEB.
- Diseño de una topología de la red de la COAC utilizando herramientas de simulación.
- Simulación de diferentes ataques los cuales son los más comunes que se obtuvo de la previa investigación.
- Aplicación de mecanismos de seguridad.
- Análisis de resultados.
- Elaboración de un manual de prevención.

CAPITULO IV

4. Resultados y Discusión

Dentro de este capítulo se plasma los resultados obtenidos de las simulaciones en tres distintos escenarios, lo que dio lugar a determinar de qué manera mejora la seguridad informática dentro de la infraestructura de red de la cooperativa, además, se muestra de qué manera proteger al servidor web de posibles ataques provenientes de internet. Para ello, se implementaron 3 escenarios:

1. Escenario antes del ataque.
2. Escenario durante el ataque.
3. Escenario aplicando los mecanismos de seguridad.

Estas simulaciones se realizaron bajo la herramienta GNS3 en la cual se diseñó la topología de red, además, permitió la utilización de dispositivos reales como routers, así como máquinas virtuales para simular los servidores web y DMZ.

4.1 Topología de red del servidor de la COAC "Riobamba".

La Figura 2, muestra el esquema real de la red de la cooperativa, el cual se tomó de base para realizar una réplica en el simulador y sobre el cual se realizó los experimentos y ataques con el fin establecer mecanismos de seguridad que ayuden prevenir y detectar ataques informáticos.

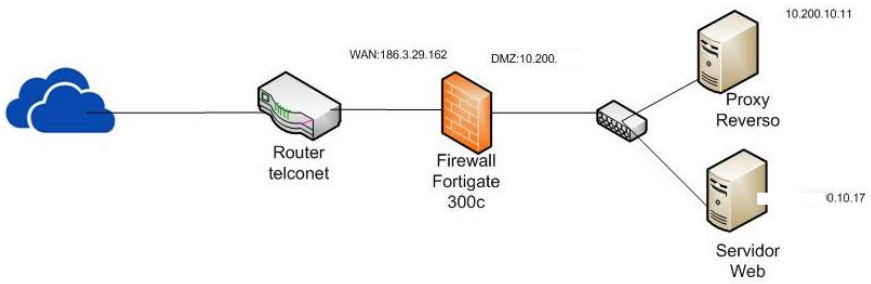


Figura 2: Topología de la red para el servidor WEB.

Como se puede visualizar en la figura 2, la topología de red de la COAC "Riobamba Ltda. Cuenta con un firewall Fortigate 300c el cual filtra todo el tráfico que entra desde el internet, sin embargo, este no es capaz de proteger de ciertos tipos de ataques que se pueden suscitar al estar expuesto el servidor web.

Al realizar el análisis de vulnerabilidades al servidor web mediante la técnica Banner Grabbing de la cooperativa se obtuvieron los resultados presentes en la Tabla 2 y 3.

Tabla 2: Vulnerabilidades encontradas en la WEB de la COAC "Riobamba Ltda."

Vulnerabilidades	Descripción	Consecuencias
CRIME SPDY	CRIME filtración de información de ratio de compresión. Es una vulnerabilidad de seguridad contra cookies web.	Permite al atacante llevar a cabo el secuestro de una sesión web autenticada, permitiendo así lanzar otros ataques.
POODLE SSL V3	Consiste en aprovecharse de una característica que hace que, cuando un intento de conexión segura falla, se proceda a intentar realizar de nuevo esa conexión pero con un protocolo de comunicación más antiguo.	Primero se fuerza el uso de un protocolo no seguro y luego se aprovecha una vulnerabilidad en él para obtener la información que antes se enviaba cifrada y un atacante no podía descifrar.
Servidor Apache 2.2.15	La versión del servidor puede llegar leta y vulnerable.	Al usar una versión antigua de apache pueden presentarse vulnerabilidades de seguridad.

WAF/IPS "desconocido"	Un firewall para protección de aplicaciones (WAF) no debe considerarse como una alternativa para los cortafuegos de red tradicionales.	Los WAF se pueden utilizar en entornos para proporcionar una protección a las aplicaciones / servidores web. Caso contrario las aplicaciones quedarían vulnerables a ciertos ataques.

Tabla 3: Resultado del escaneo de puertos en el servidor Web de la COAC "Riobamba

Puerto	Estado	Protocolo
21	Abierto	Pop3 (e-mail)
80	Abierto	HTML (Web)
110	Abierto	Pop3 (e-mail)
143	Abierto	IMAP4 (e-mail)
443	Abierto	HTTPS/SSL
113	Cerrado	Pop3 (e-mail)

4.2 Escenario antes del ataque.

La Figura 3, muestra el escenario simulado en GNS3 de la topología de red de la cooperativa en él se simula las transacciones típicas en un día normal de actividades, esta simulación se lleva a cabo con el fin de medir los tiempos de respuesta del servidor web, el uso de CPU y el uso de memoria RAM.

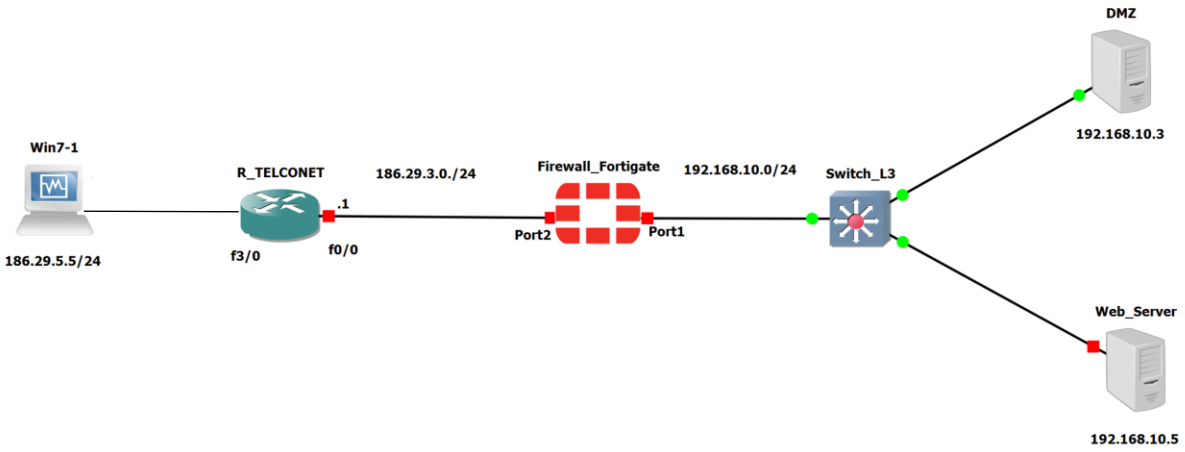


Figura 3: Topología antes el ataque.

En las Figuras 4, 5 y 6 se muestran los resultados del uso de los recursos del servidor en un estado normal, es decir, sin ningún tipo de ataque y con la concurrencia típica en diferentes días.

Se midieron distintos parámetros como son: tiempos de respuesta del servidor web, uso del CPU y el uso de memoria RAM. Estos datos se tomaron en los periodos previamente establecidos.

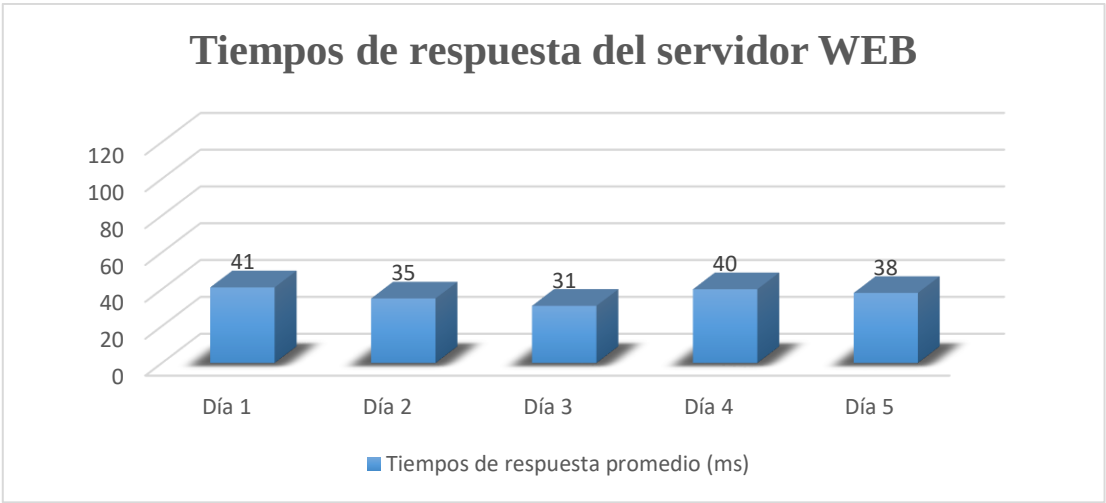


Figura 4: Tiempos de respuesta del servidor web.

La Figura, 4 muestra los tiempos de respuesta del servidor tomados desde un usuario, se puede notar que el tiempo de respuesta más alto es de 41 milisegundos, en el día 1 de pruebas, a pesar

de ser el valor más alto es bastante aceptable para poder usar con normalidad los servicios de la página web por lo que se considera que los usuarios tendrán una experiencia agradable al usar la web.

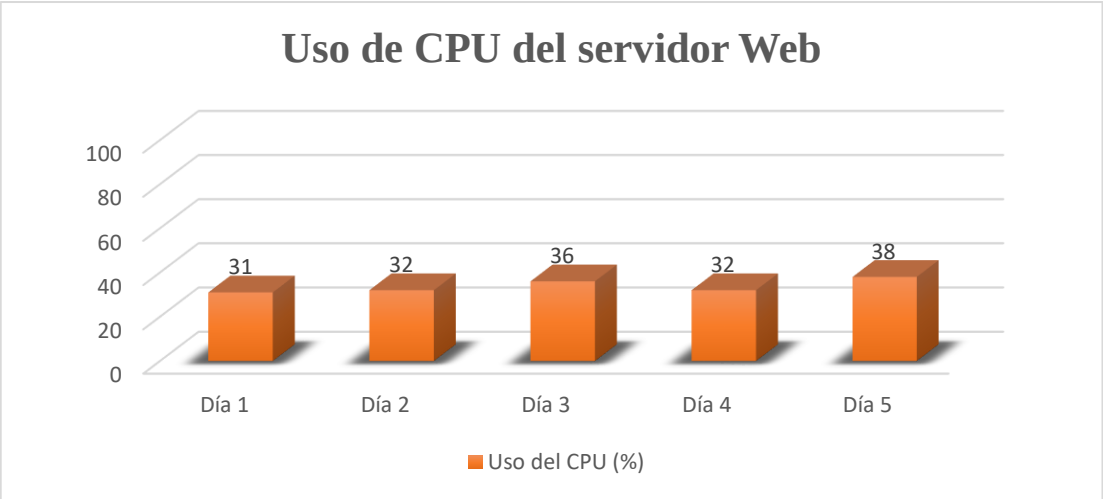


Figura 5: Uso del CPU del servidor Web.

Por otro lado, la Figura 5, muestra el comportamiento del CPU por parte del servidor WEB en este apartado se concluye que el uso de CPU es estable sin uso excesivo siendo el valor más alto 38% en el día 4.

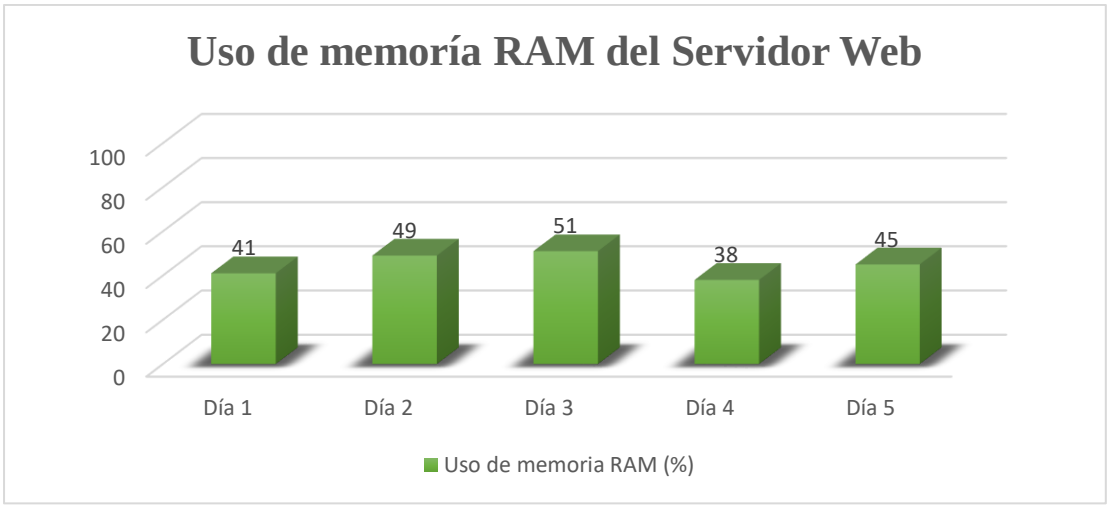


Figura 6: Uso de la memoria RAM del servidor Web.

La Figura 6, muestra el uso de memoria RAM, la máquina virtual usada para el servidor Web tiene asignada 2048 Mb de memoria, como se puede observar el pico máximo de uso es de 51% ejecutando los procesos del servidor Web.

4.3 Escenario durante el ataque

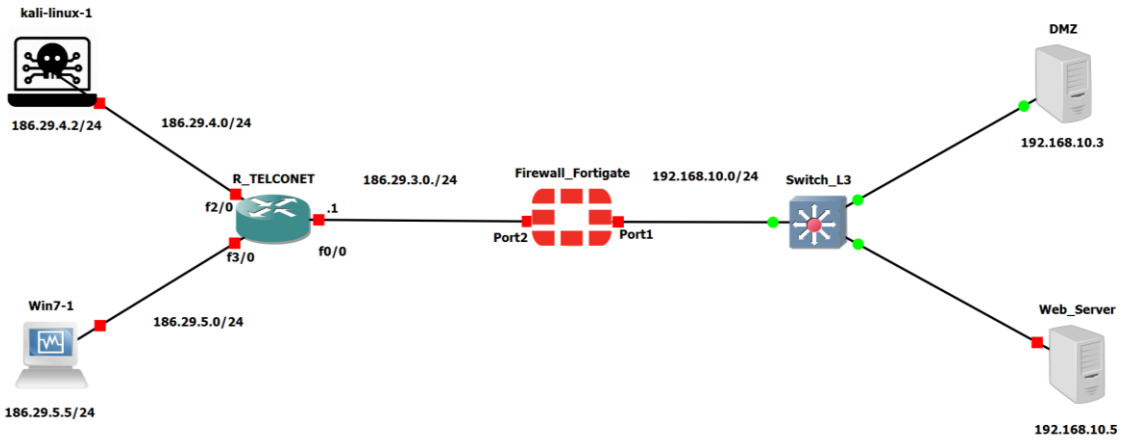


Figura 7: Escenario durante el ataque

En la Figura 7, se observa la topología de red utilizada para simular un ataque al servidor web de la cooperativa en donde el atacante está representado con una máquina virtual con el S.O Kali Linux el cual tiene las herramientas necesarias para poder realizar diversos ataques al servidor con el fin de conocer cómo reacciona este y poder tomar las medidas necesarias para poder mitigar cualquier vulnerabilidad existente.

En la Tabla 4, se visualiza los tipos de ataques al cual se sometió el servidor web, se utilizaron estos tipos de ataques ya que son los más comunes en este tipo de escenarios según la información recolectada y brindada por los técnicos del departamento de sistemas de la COAC Riobamba. Sin embargo, cabe destacar que al estar en un escenario virtual ciertos de los ataques no pueden tener el mismo impacto que al estar dentro del escenario real. Por lo que, los resultados pueden diferir.

Tabla 4: Tipos de ataques efectuados al servidor web.

Ataque	**Herramienta**
SYN Flood	Ettercap
Escaneo de puertos	Zenmap
Cross-Site Request	WireShark
Banner Grabbing	Nmap

Con el servidor bajo los ataques se midieron 3 tipos de parámetros los cuales son: tiempos de respuesta, uso del CPU y el uso de memoria RAM.

4.3.1 Resultados bajo ataques

Como se puede apreciar en la figura 8, los tiempos de respuesta bajo un ataque varían en cierta medida a los tiempos presentados en la Figura 4 donde el servidor no tiene ningún tipo de presión. Tras realizar los ataque mediente diversas herramientas de Kali Linux se observa que los tiempos de respuesta incrementan ya que el sevidor esta recibiendo varias peticiones simultaneamente por lo que utiliza más recursos y por consecuencia el tiempo de respuesta se incrementa es más notable en el periodo diurno ya que es donde más concurrencia tiene el servidor.

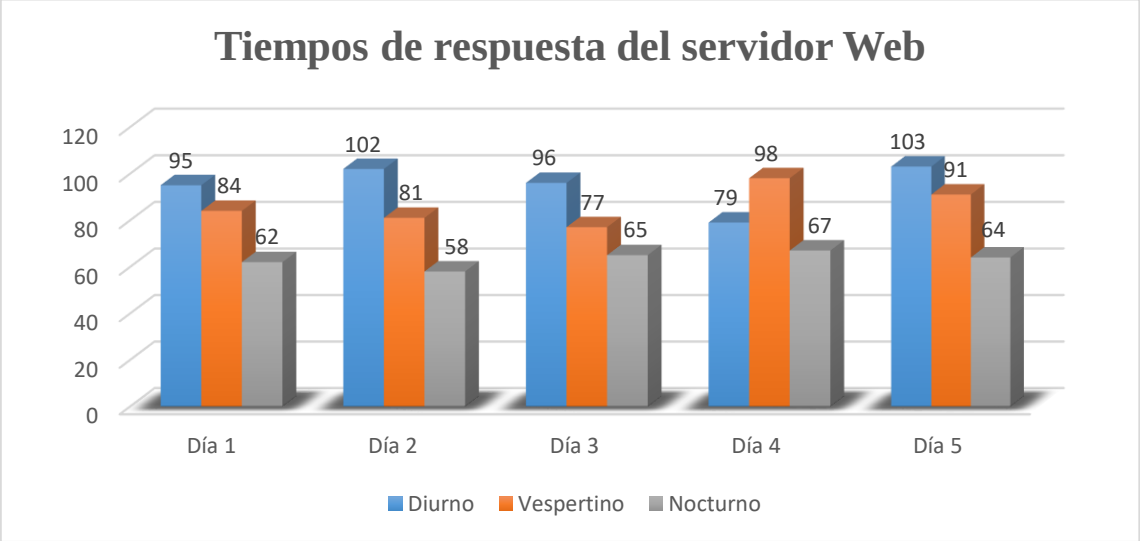


Figura 8: Tiempos de respuesta del servidor bajo ataque.

En la Figura 9, se observa el uso del CPU por parte del servidor web, se pude apreciar que por las mañanas el uso es más elevado llegando a sobrepasar el 80% en el 3er día por el constante su uso de recuros al estar bajo ataques de **SYN Flood** que inunda de peticiones al servidor web.

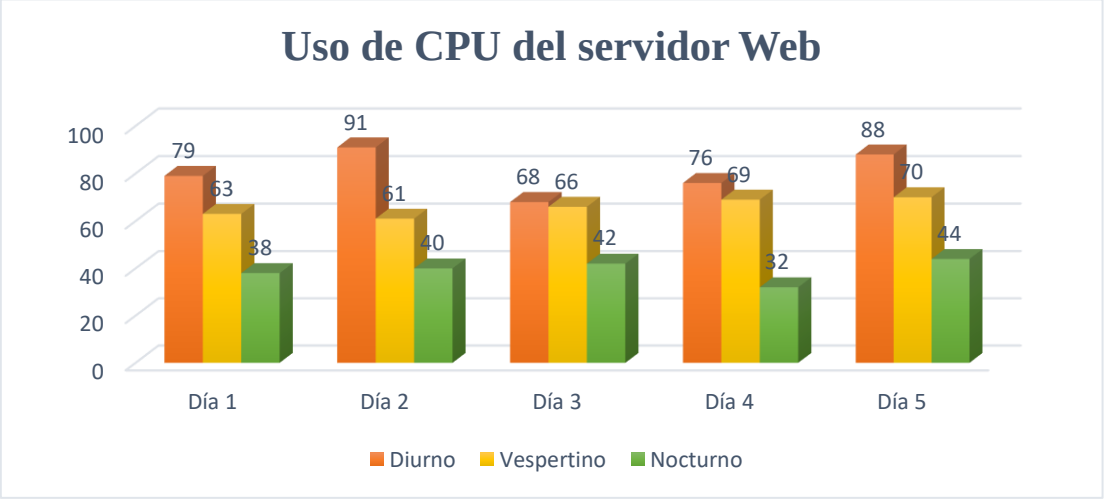


Figura 9: Uso del CPU del servidor Web bajo diversos ataques.

La Figura 10 muestra el uso de memoria RAM del servidor Web la cual tiene asignada 2048 Mb como se puede apreciar el uso de memoria no es tan extenso siendo el valor más alto 58% en el día 4 por el turno diurno.

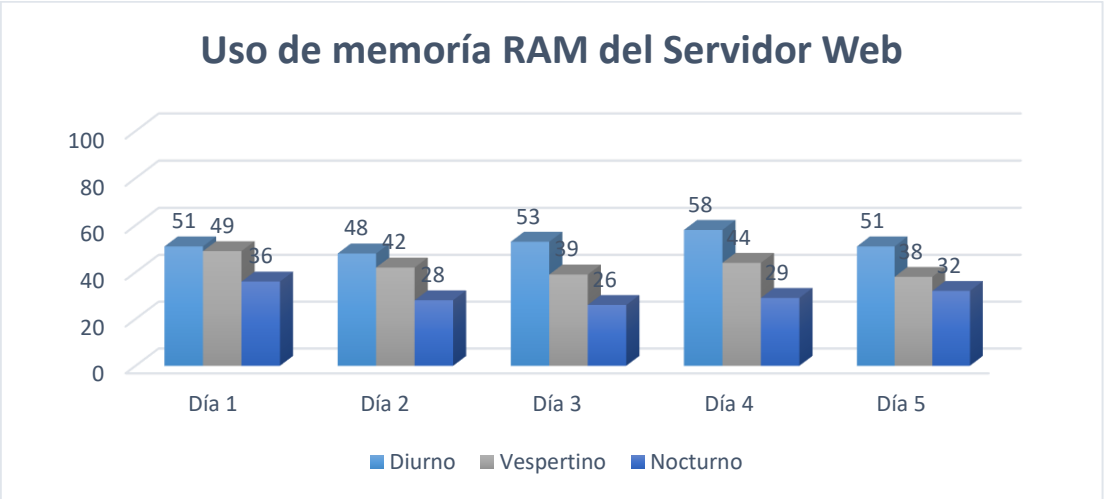


Figura 10: Uso de memoria RAM del servidor Bajo diversos ataques.

4.3.2. Resultados de los escaneos de puertos abiertos

La Tabla 5, muestra el resultado de puertos abiertos/cerrados en el servidor web mediante la utilización de Zenmap la cual se ejecutó desde Kali Linux, como se puede apreciar existen varios puertos lo que representa un nivel de amenaza para el servidor moderado, se realizó un análisis para determinar cuál sería la configuración más óptima.

Tabla 5: Resultado del escaneo de puertos en el servidor bajo ataque simulado.

Puerto	Estado	Protocolo
21/tcp	Abierto	Pop3 (e-mail)
80/tcp	Abierto	HTML (Web)
110/tcp	Abierto	Pop3 (e-mail)
143/tcp	Abierto	IMAP4 (e-mail)
443/tcp	Abierto	HTTPS/SSL
113/tcp	Cerrado	Pop3 (e-mail)

4.4. Escenario aplicando mecanismos de seguridad.

En este tercer escenario, se agregaron a la simulación los mecanismos de defensa. Estos se implementaron con el fin de mejorar la seguridad informática en la infraestructura de red de la COAC "Riobamba" Ltda. Se demuestra que la seguridad frente al servidor web mejora de manera sustancial como se puede apreciar en la Tabla 6 y en las Figuras 12, 13 y 14 donde se detalla de mejor manera los resultados obtenidos de la simulación aplicando mecanismos de defensa.

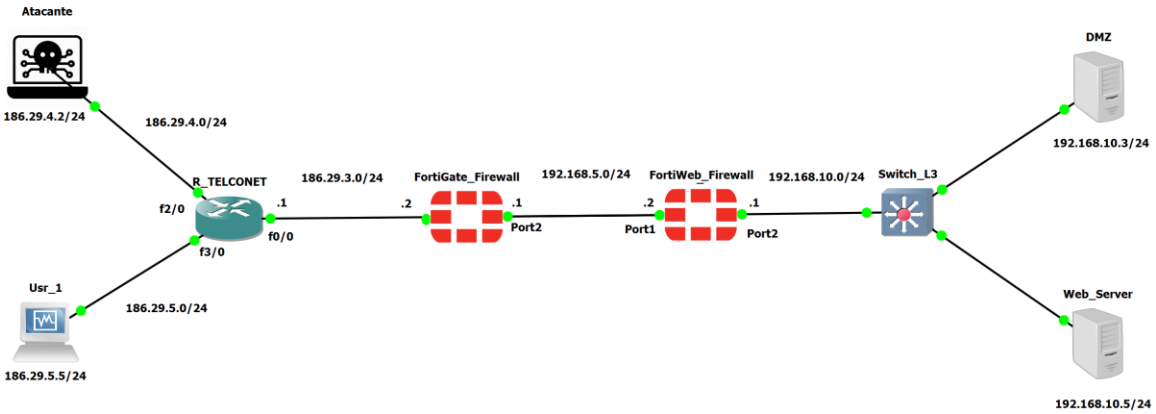


Figura 11: Topología de la red aplicando los mecanismos de defensa.

En la Figura 11, se observa la topología de red donde se implanto un segundo firewall **FortiWeb** detrás del **FortiGate**, este funciona como un WAF (Web Application Firewall) que se diferencia de un firewall normal ya que puede filtrar el contenido de aplicaciones web específicas, mientras que un firewall de red protege el tráfico entre los servidores. Al inspeccionar el tráfico HTTP un WAF protege a las aplicaciones web contra ataques como los de inyección SQL, XSS y falsificación de petición de sitios cruzados (Miguel, 2016). Por lo que es recomendado para mejorar la seguridad lógica en la red de la COAC “Riobamba” Ltda. De igual manera se puso al servidor bajo ataques informáticos determinar cómo reacciona ante estas situaciones durante 5 días en los horarios anteriormente mencionados.

4.4.1. Resultados de escaneo de puertos con mecanismos de defensa.

La Tabla 6, muestra el resultado del escaneo de puertos después de haber aplicado mecanismos de seguridad, se puede observar que al contrario de lo que muestra la Tabla 5, los puertos 21 y 110 ahora se encuentras cerrados, resultado del filtrado realizado por el segundo firewall FortiWeb.

Dichos puertos 21 y 110 son usados para transmisión de información FTP y Pop3 respectivamente mantener estos puertos abiertos puede suponer una amenaza para el servidor web.

Tabla 6: Resultados de puertos abiertos/cerrados aplicando protocolos.

Puerto	Estado	Protocolo
21/tcp	Cerrado	FTP
80/tcp	Abierto	HTML (Web)
110/tcp	Cerrado	Pop3 (e-mail)
143/tcp	Abierto	IMAP4 (e-mail)
443/tcp	Abierto	HTTPS/SSL
113/tcp	Cerrado	Pop3 (e-mail)

4.4.2. Uso de recursos del servidor Web y tiempos de respuesta.

Como se observa en la Figura, 12 los tiempos de respuesta del servidor aplicando los mecanismos de seguridad mientras está bajo ataque son más bajos, siendo el más alto 92 ms (Milisegundos) en el día 5 en el turno Vespertino. Estos tiempos de respuesta hace que los usuarios que acceden al servidor mediante la web tengan una experiencia más ágil en navegación y consumo de información.

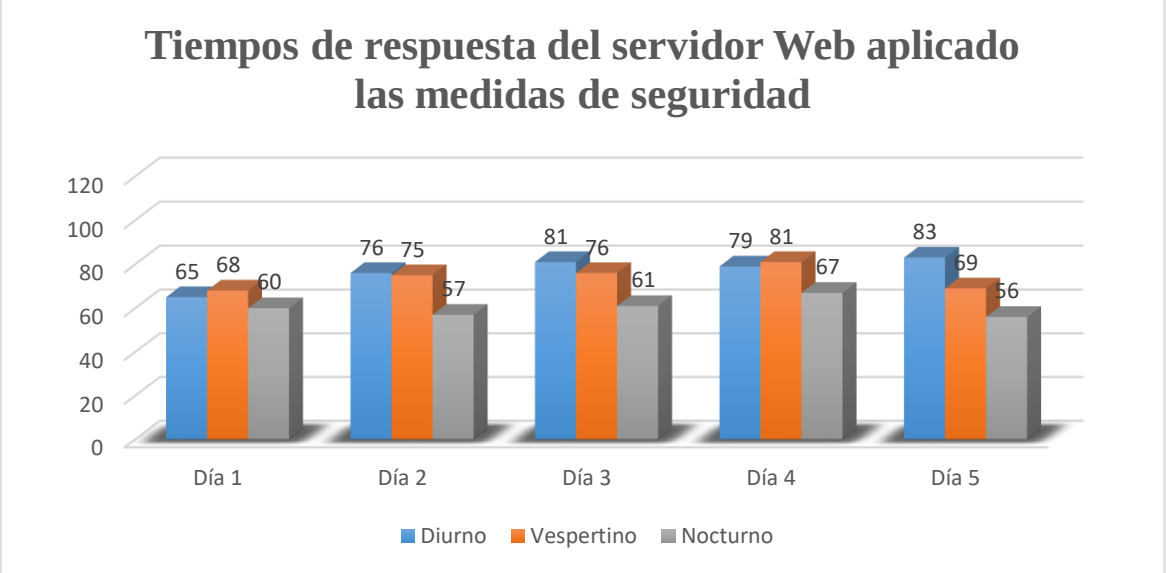


Figura 12: Tiempos de respuesta con protocolos de seguridad.

Dentro de la Figura 13, se puede visualizar el comportamiento del CPU por parte del servidor web el cual presenta un menor siendo el pico más alto 64% uso ya que el firewall al filtrar tráfico procedente desde el atacante.

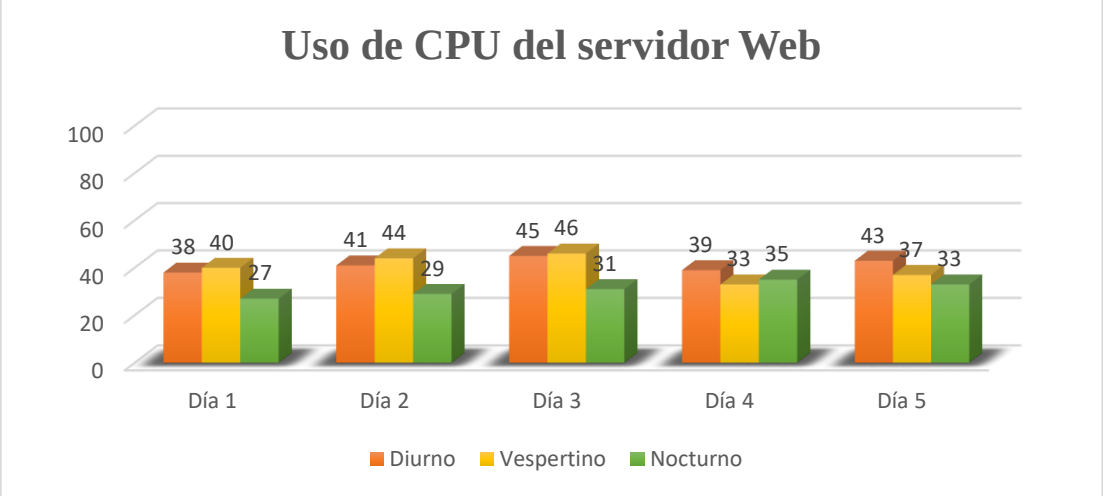


Figura 13: Uso del CPU con protocolos de seguridad.

Con la memoria RAM sucede algo similar; en la Figura 14 se puede observar que el uso de memoria disminuye en 16% en comparación a cuando la red está bajo ataque y sin mecanismos de defensa ya que el servidor se encuentra bajo menos presión y se evidencia que el firewall FortiWeb esta filtrado los ataques.

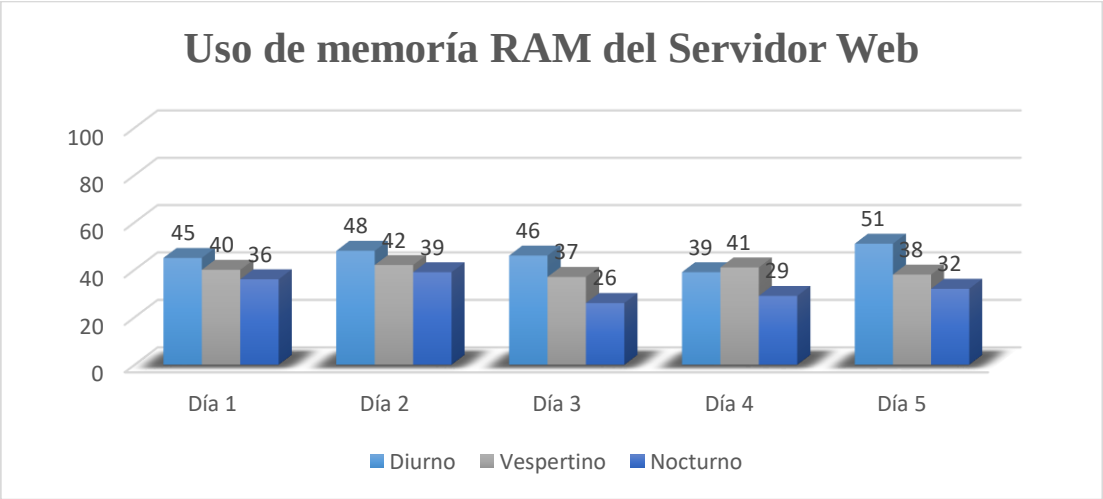


Figura 14: Uso de memoria RAM con protocolos de seguridad.

4.5 Análisis de resultados

Tabla 7: Cuadro comparativo de resultados

	SIN MECANISMOS DE SEGURIDAD BAJO ATAQUES			CON MECANISMOS DE SEGURIDAD BAJO ATAQUES		
	Tiempos de Respuesta	**Uso de CPU**	**Uso de Menoría RAM**	**Tiempos de Respuesta**	**Uso de CPU**	**Uso de Menoría RAM**
Día 1	80 (ms)	60%	45%	64 (ms)	35%	40%
Día 2	80 (ms)	64%	39%	69 (ms)	38%	43%
Día 3	97 (ms)	58%	39%	72 (ms)	40%	36%
Día 4	81 (ms)	59%	43%	72 (ms)	35%	36%
Día 5	86 (ms)	67%	40%	73 (ms)	37%	40%

La Tabla 7 muestra la comparación del uso de recursos del servidor web CPU y memoria RAM, así como también los tiempos de respuesta, cuando no existen dichos mecanismos y cuando se aplican dentro del ambiente simulado, estos datos se resumen y comparan en las Figuras 15 y 16, respectivamente.

Figura 15: Comparación tiempos de respuesta

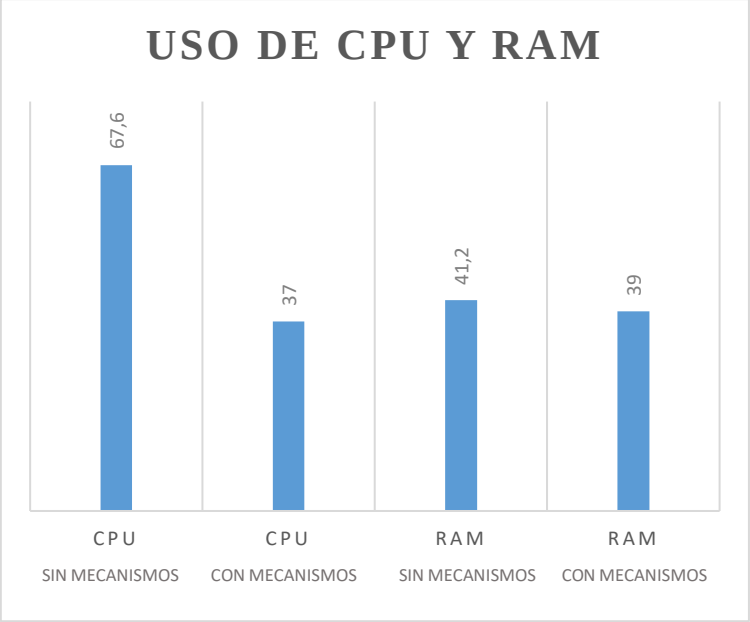


Figura 16: Comparación uso de recursos del servidor WEB

CONCLUSIONES

- Al analizar las vulnerabilidades existentes en la Web de la Cooperativa de Ahorro y Crédito "Riobamba" Ltda., se evidencia que tiene ciertas falencias en cuanto a seguridad informática, como son: puertos TCP/IP abiertos, SLL, SPDY y la carencia de un Firewall de aplicaciones (WAF) lo cual permitió determinar cuáles son los puntos a mejorar para tener una infraestructura de red más segura dentro de la cooperativa.
- La evaluación de las vulnerabilidades existentes en la infraestructura de red de la cooperativa demostró que si se llegará a suscitar un ataque este tendría consecuencias graves tanto en la disponibilidad del servidor como en la integridad de la información.
- Los ataques informáticos realizados dentro del escenario simulado determinaron cómo reacciona la infraestructura de red, así como el servidor web para establecer los mecanismos de seguridad necesarios a considerar con el fin de mejorar la topología de red de la COAC "Riobamba" Ltda.
- La implementación de los mecanismos de seguridad en el ambiente simulado demostró que los tiempos de respuesta se redujeron de 84.8 milisegundos a 70 milisegundos, así como también, se redujo el uso de recursos del servidor web, uso CPU del 61.6% paso al 37% y el uso de memoria RAM del 41.2% al 39%, lo que permitió de esa manera mejorar la fluidez en el tráfico de datos y, sobre todo, optimar la seguridad informática para mantener la integridad, autenticidad y disponibilidad de la información alojada en el servidor web.
- El manual de usuario tiene como finalidad guiar en la configuración de protocolos de seguridad específicamente de un firewall especializado o WAF para prevenir ataques al servidor web, los resultados pueden variar dependiendo de la infraestructura donde se apliquen.

RECOMENDACIONES

- Realizar una valoración del estado de la seguridad informática dentro de la infraestructura de red de la Cooperativa con el fin de estar siempre actualizados y prevenidos ante cualquier eventualidad.
- La implementación de un WAF o firewall de aplicaciones es un paso fundamental no solo para mejorar la seguridad informática dentro de la institución financiera, sino también para abrir camino hacia la evolución como la implementación de la banca móvil.
- Tomar en cuenta que, así como los mecanismos de seguridad evolucionan los ciberataques también lo hacen, es por ello, importante el estar preparados y actualizados para prevenir un ataque informático y con ello alteraciones en la información o datos de suma importancia para la cooperativa, sus socios y su comunidad en general.
- Capacitar a los usuarios finales de los aplicativos web, en el uso y correctas costumbres para evitar ser víctimas de un ataque informático de cualquier índole ya que al estar expuestos al internet existe una mayor probabilidad de ser víctimas de una cibercriminal

5. BIBLIOGRAFÍA

Bezzi, G. P. (2016). Análisis de botnets y ataques de. *ESET*, 12.

Catoira, F. (21 de Noviembre de 2017). *welivesecurity ESET*. Obtenido de https://www.welivesecurity.com/la-es/2012/11/21/obtener-informacion-de-servidores-web-con-banner-grabbing/

Cordero, M. (2016). Detección y mitigación de ataques ARP Spoof empleando entornos virtualizados. *Geeks Tendencias en Computación*, 7.

Giacobbi, G. (2016). *GNU Netcat project*. Obtenido de http://netcat.sourceforge.net/

Herjavec Group. (2017). *HCybersecurity Ventures.* Steve Morgan, Editor-in-Chief.

ISOTools Excellence. (26 de Enero de 2017). *Blog especializado en Sistemas de Gestión*. Obtenido de https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Jiménez, C. J. (2016). *Seguridad en redes y sistemas: Técnicas y conceptos sobre.* España.

López, P. A. (2016). *Seguridad Informática.* Editex.

Luz, S. D. (18 de Enero de 2014). *RZ Redes Zone*. Obtenido de https://www.redeszone.net/2014/01/18/zenmap-la-interfaz-grafica-oficial-de-nmap-para-escanear-puertos-a-fondo/

Miguel, j. T. (2016). *Implantación de aplicaciones web en entornos internet, Intranet y Extranet.* Edisiones Paraninfo S.A.

Muñoz, F. R. (2018). *T´ecnicas para la Optimizaci´on del.* Madrid.

NMAP.ORG. (2015). *Nmap Security Scanner*. Obtenido de NMAP: https://nmap.org/

Organización de los Estados Americanos. (2018). *Estaod de la Cibersegurdad en el Sector Bancario en América Latina y el Caribe.* Mexico : OEA.

Racciatti, H. M. (2016). *Técnicas de SQL Injection.* Argentina.

Silvia M. Quiroz-Zambrano, D. G.-V. (2017). Seguridad en informática: consideraciones. *Revista Científica Dominio de las Ciencias*, 676-688.

SniferLabs. (2016). *SniferLabs*. Obtenido de https://www.sniferl4bs.com/2016/01/hacking-101-conociendo-y-aprendiendo.html

Vieites, Á. G. (2016). TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS. *EDISA*, 13.

Vvasquez, Y. D. (2018). ANÁLISIS E IDENTIFIACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD. *UNAD*, 60.

ANEXOS

Anexo A: Escenarios de la investigación.

1.1 Escenario de la COAC "Riobamba Ltda. Esquema del servidor WEB.

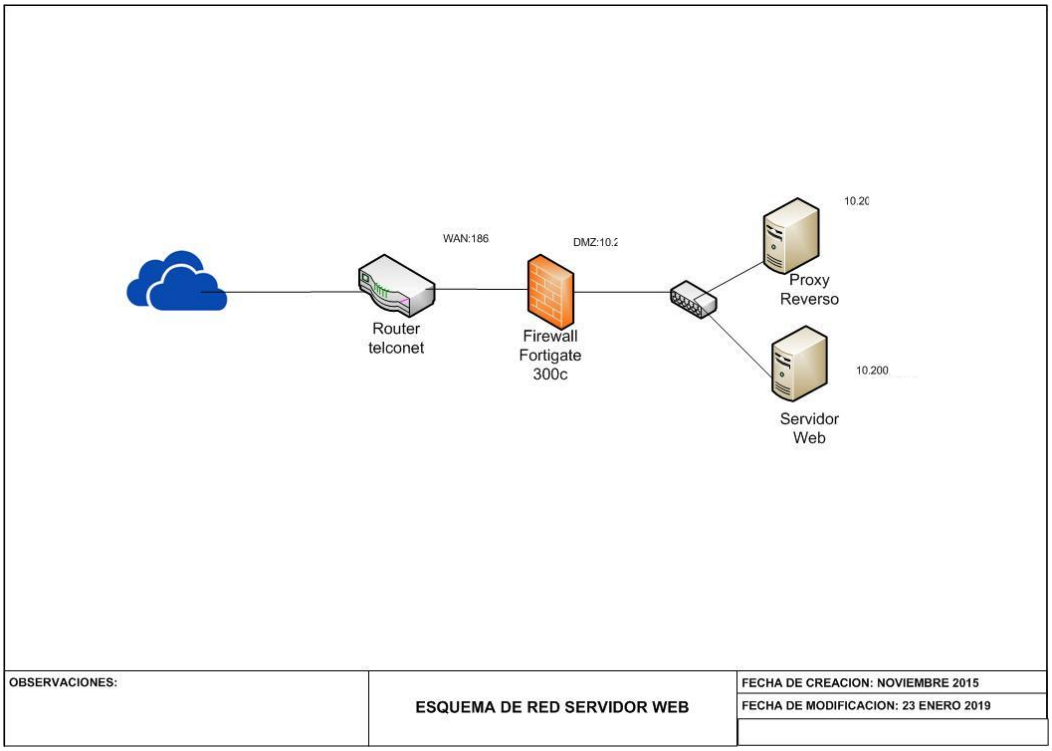


Figura 17: Esquema de red servidor WEB COAC "Riobamba" Ltda.

FUENTE: COAC "Riobamba" Ltda.

Como se puede visualizar en la figura 17, la topología de red de la COAC "Riobamba Ltda., cuenta con un firewall Fortigate 300c el cual filtra el tráfico que entra desde el internet, sin embargo, este no es capaz de proteger de ciertos tipos de ataques que se pueden suscitar al estar expuesto el servidor web. Este esquema fue entregado por los técnicos de la cooperativa.

1.1 Escenario de la COAC con su topología y un ataque externo

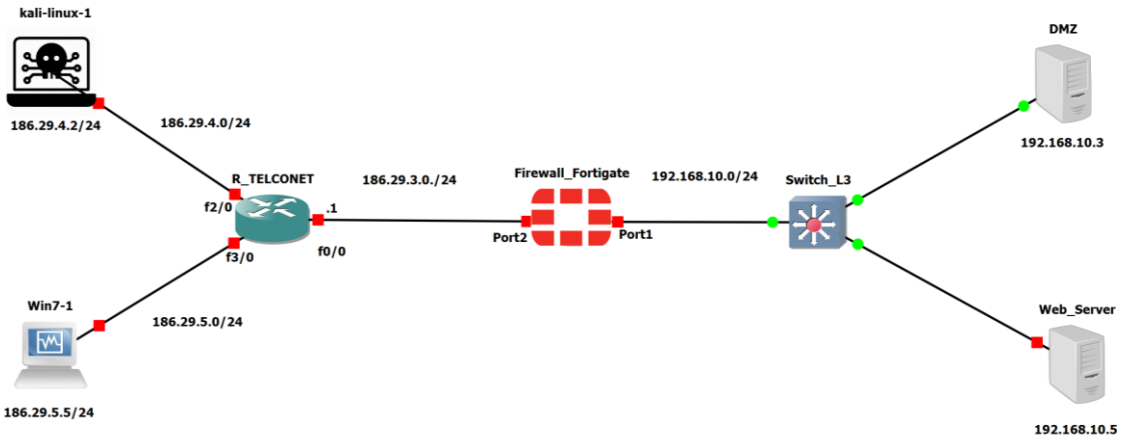


Figura 18: Topología del servidor WEB bajo un ataque

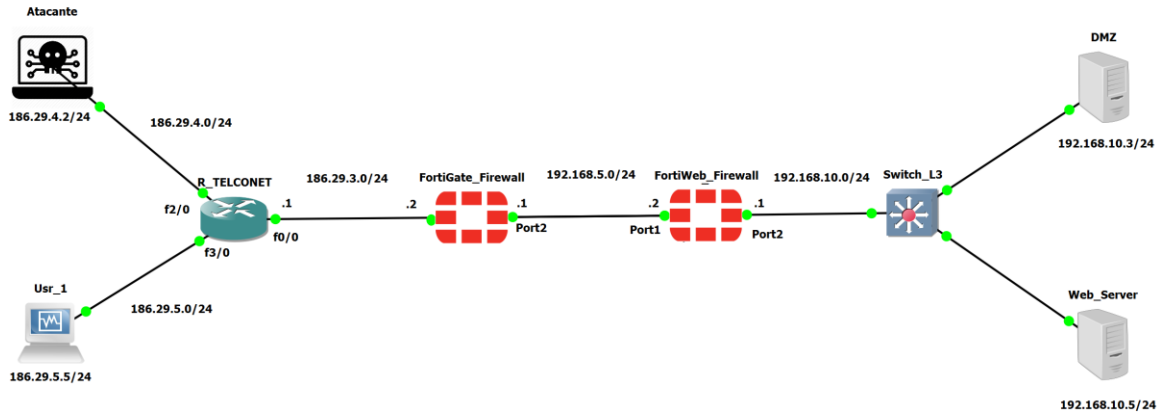


Figura 19: Topología de la red aplicando mecanismos de seguridad.

En la figura 18, se observa la topología implementada para simular un ataque al servidor web usando como atacante una máquina virtual con Kali Linux, mientras en la figura 19, se observa el escenario implementado mecanismos de seguridad.

Anexo B: Máquinas virtuales usadas para la simulación

2.1 Máquina virtual Kali Linux

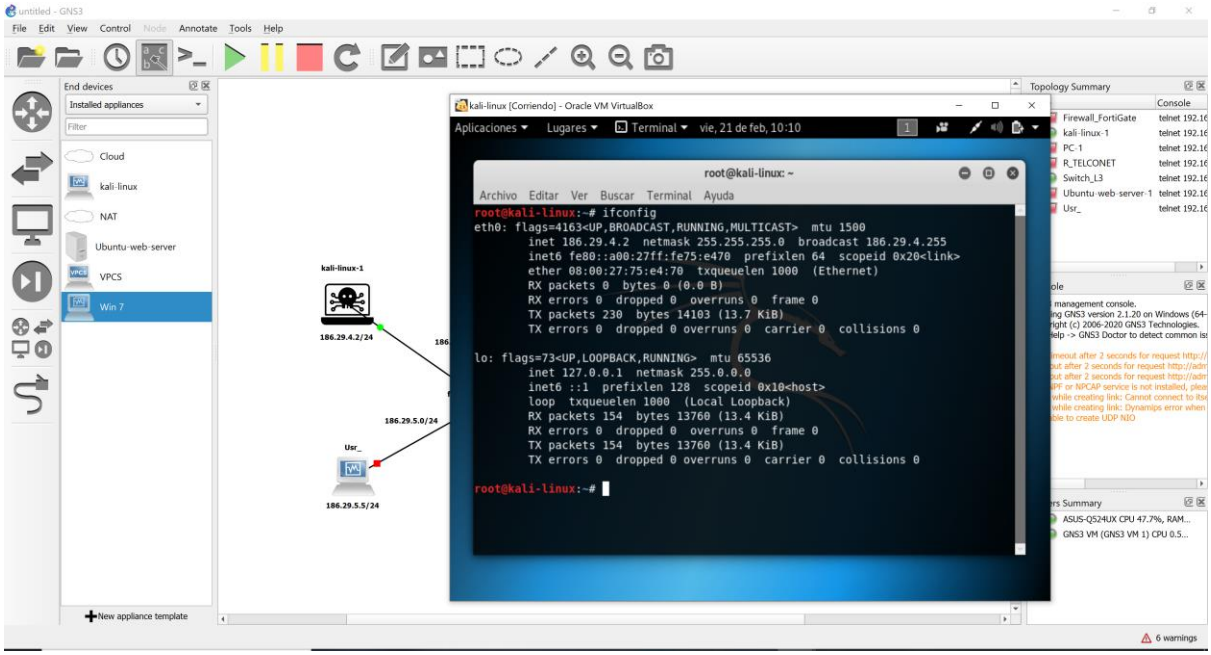


Figura 20: Captura de pantalla de la VM Kali Linux

En la figura 20, se observa la máquina virtual Kali Linux en la cual se configuraron los ataques hacia el servidor web, esta máquina tiene asignado un procesador Intel Core i7 con 2 núcleos y 2048 de RAM.

2.2 Máquina Virtual con Ubuntu Server

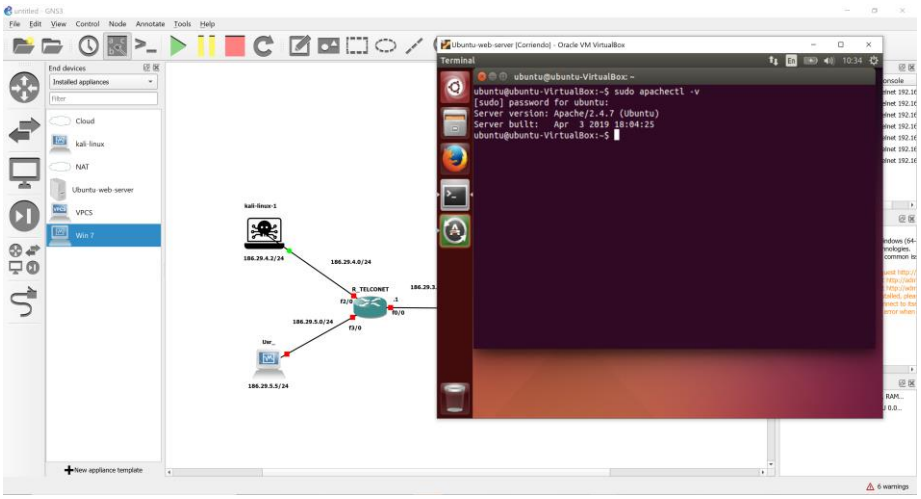


Figura 21: Captura de pantalla de la VM Servidor Web.

En la figura 21. Se aprecia una captura de pantalla del servidor web el cual está alojado en Ubuntu server 14.04 cuenta un procesador Intel Core i7 con 2 núcleos y 2048 de RAM. Dentro de este servidor de igual manera se configuro un servidor DNS para resolver peticiones a la url: *cooprio.fin.ec*. De esta manera se simulo el esquema de red del servidor WEB de la COAC "Riobamba" Ltda.

Anexo C: Routers usados en la simulación

3.1 Router Telconet

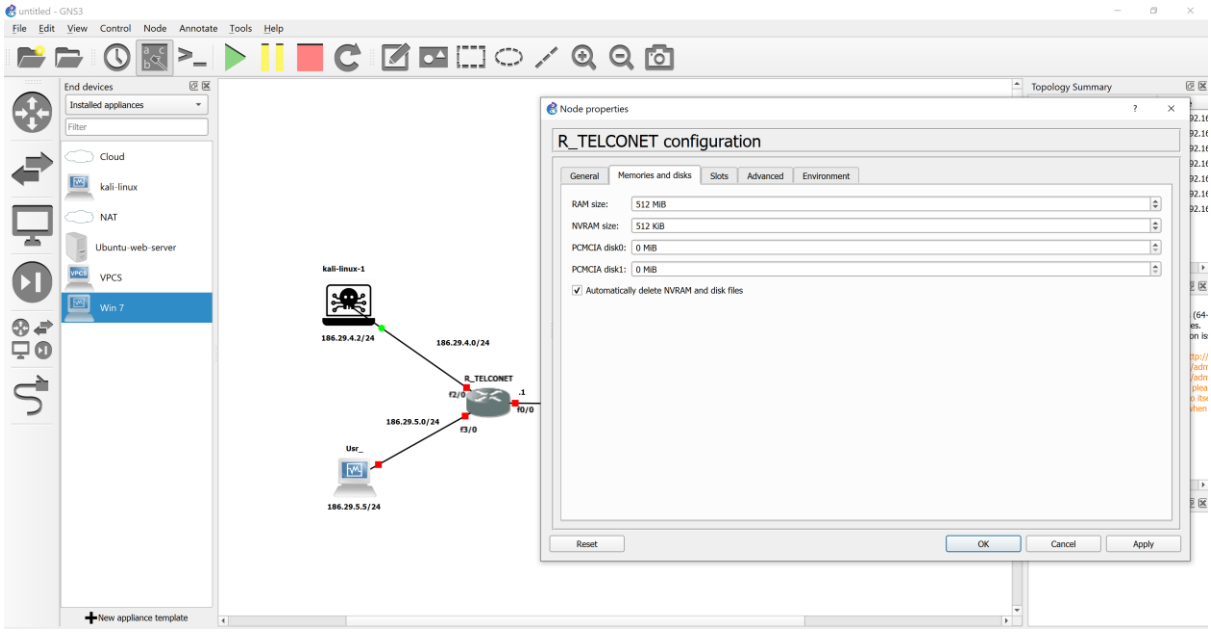


Figura 22: Captura de pantalla de R_Telconet

La figura 22, muestra la configuración del router de Telconet el cual hace de salida al internet en el escenario simulado está conectado a Kali Linux y a un usuario que para realizar mediciones.

3.2 Firewall Fortigate

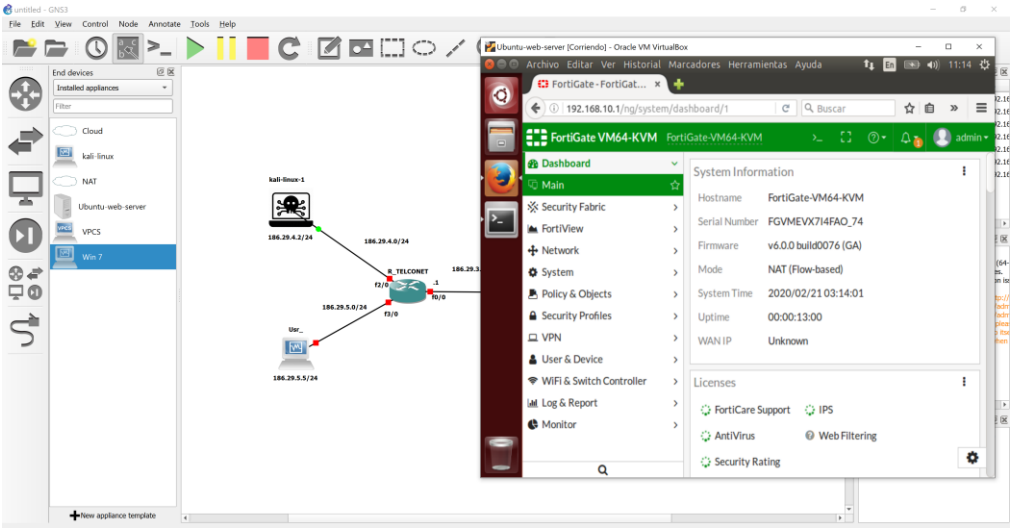


Figura 23: Captura de pantalla del Firewall FortiGate

En la figura 23, se observa las características del Firewall FortiGate el cual se usó para la simulación del escenario, dicho router tiene 5 interfaces Gigabit Ethernet, 1024 MB de RAM y 1 vCPU. Es un firewall muy completo para proteger la red ya que en su apartado de seguridad tiene varias herramientas de seguridad como se aprecia en la figura 24.

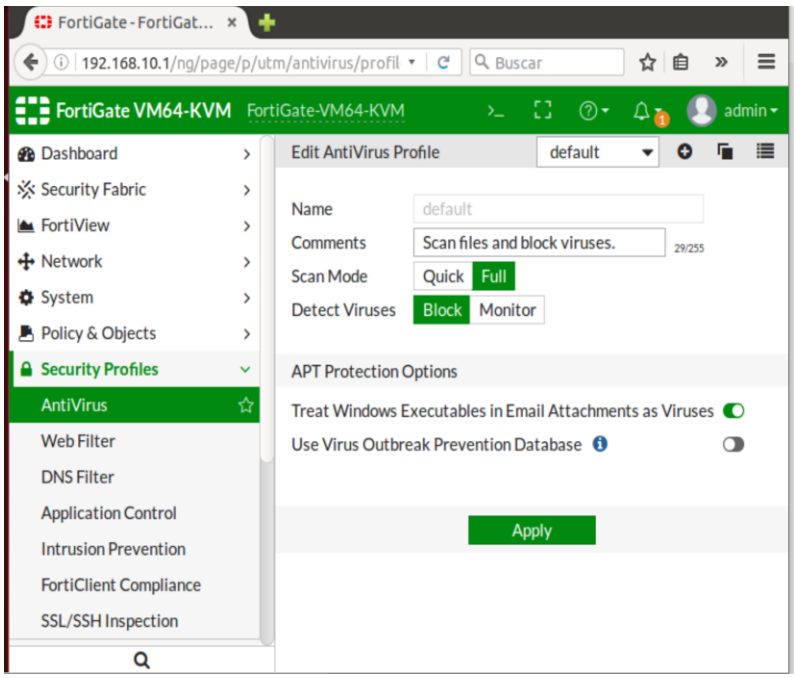


Figura 24: Captura de pantalla seguridades fortigate.

3.3 Firewall Fortiweb

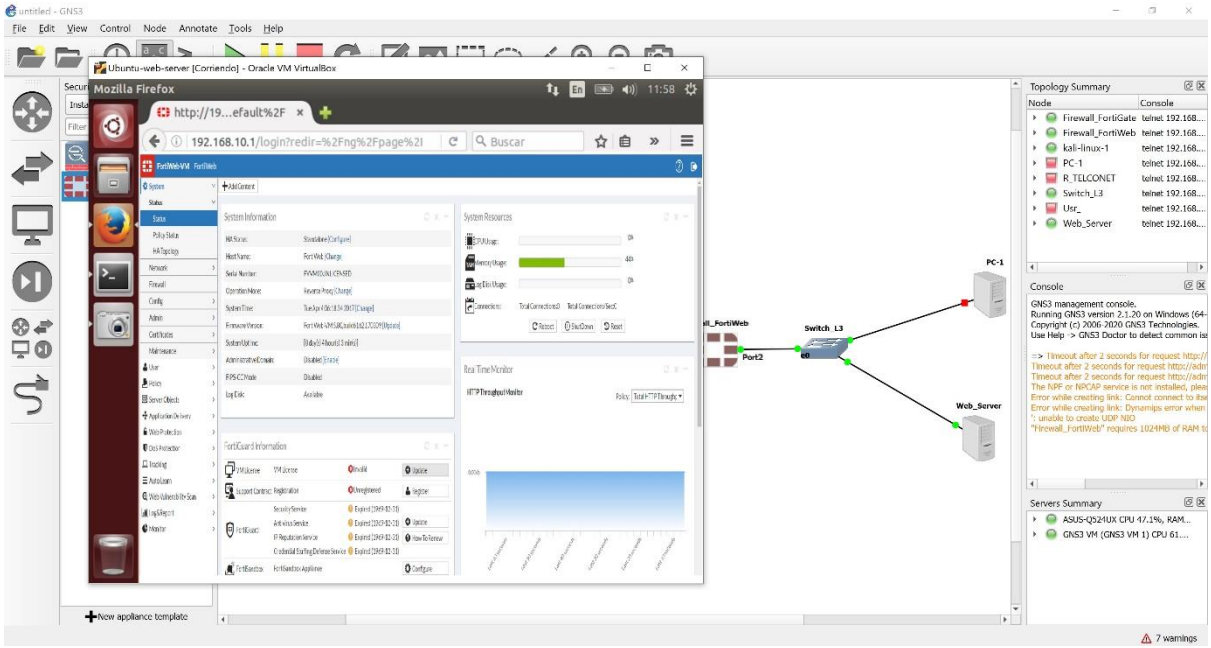


Figura 25: Captura de pantalla del firewall FortiWeb.

La figura 25, muestra la pantalla principal del FortiWeb usado para la simulación este router tiene 5 interfaces Gigabit Ethernet, 1024 MB de RAM y 1 vCPU. Este firewall cuenta con herramientas de protección completa y especializada a todos los niveles para las aplicaciones y servicios Web. Algunas de las características de seguridad que ofrece son:

- Cross-Site Scripting (XSS).
- Cross-Site Request Forgery (CSRF).
- Insecure Cryptographic Storage.
- Failure to Restrict URL Access.

Anexo D: Tabla de IPs usadas en la simulación

4.1 Configuraciones usadas dentro de la simulación

Tabla 8: Hosts, Interfaces e Ips usadas en la simulación

IP	INTERFACE	HOST
186.29.3.1/24	F0/0	R_TELCONET
186.29.3.2/24	Port1	FortiGate_Firewall
186.29.4.1/24	F2/0	R_TELCONET
186.29.4.2/24	Eth0	Kali Linux
186.29.5.1/24	F3/0	R_TELCONET
186.29.5.2/24	Eth0	Usr_1
192.168.5.1/24	Port2	FortiGate_Firewall
192.168.5.2/24	Port1	FortiWeb_Firewall
192.168.10.1/24	Port2	FortiWeb_Firewall
192.168.10.3/24	Eth0	Servidor DMZ
192.168.10.5/24	Eth0	Servidor WEB

Para la simulación del escenario se usó las ips que se muestran en la tabla 8, se implantaron en base a la configuración mostrada en el esquema de la COAC “Riobamba” Ltda. Se modificaron y adaptaron para ejemplificar de la mejor manera posible en la simulación sin que haya alteraciones en la topología original.

Anexo E: Acta de entrega recepción del manual.

DIRECCIÓN ACADÉMICA
VICERRECTORADO ACADÉMICO

SGC
SISTEMA DE GESTIÓN DE LA CALIDAD

UNACH-RGF-01-04-02.14

ACTA ENTREGA RECEPCIÓN

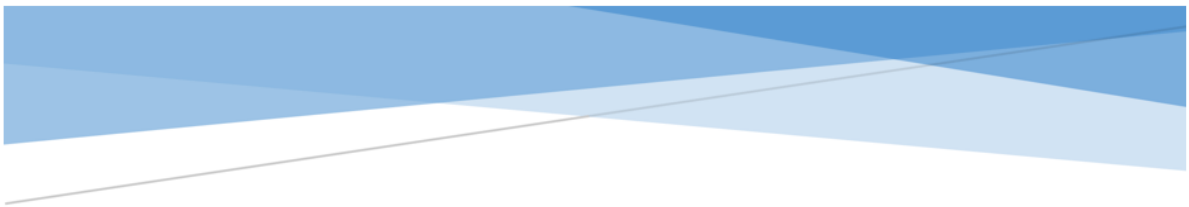
MANUAL PARA MEJORAR LA SEGURIDAD EN LA WEB DE LA COAC "RIOBAMBA" LTDA.

En la ciudad de Riobamba, a los 26 días del mes de febrero de 2020, el estudiante Francisco Manuel Pérez Rosero realiza la entrega del manual para mejorar la seguridad en la Web de la COAC "Riobamba" Ltda. Después de realiza el proyecto de investigación titulado: **DETECCIÓN Y EVALUACIÓN DE VULNERABILIDADES EN LA WEB CON LA TÉCNICA BANNER GRABBING EN LA COOPERATIVA DE AHORRO Y CRÉDITO "RIOBAMBA" LTDA.** Al Ingeniero Javier Vacacela jefe del departamento de TI de la institución, con el objetivo de dar constancia en la Entrega Recepción de conformidad del trabajo realizado.

ENTREGUÉ CONFORME
Francisco Pérez

RECIBÍ CONFORME
Ing. Javier Vacacela

Anexo F: Manual de implementación mecanismos de seguridad.



MANUAL PARA MEJORAR LA SEGURIDAD INFORMÁTICA EN EL SERVIDOR WEB DE LA COOPERATIVA DE AHORRO Y CRÉDITO "RIOBAMBA" LTDA.

Universidad Nacional de Chimborazo
Realizado por: Francisco Pérez Rosero
Riobamba - Ecuador
2020

CONTENIDO

INTRODUCCIÓN

Debido a la globalización y el avance de la tecnología, la información ha tomado un papel muy importante en cualquier organización. Además, debido al avance tecnológico, todas las organizaciones se han visto en la necesidad de adaptarse y sistematizar su información. Es por esto que en todo el mundo ocurren diferentes tipos de ataques informáticos a diario, lo que puede llevar a daños y alteraciones en la información. Esto conlleva a un gran problema ya que actualmente la información se ha convertido en uno de los activos más importantes de las organizaciones y al verse afectada puede causar daños económicos irreparables.

Por otra parte, el impacto y costo del cibercrimen sigue en aumento. Un informe realizado por Cybersecurity señala que en 2021 habrá 3.5 millones de nuevos puestos de trabajo en ciberseguridad. Sin embargo, las previsiones de empleos en seguridad cibernética no han podido seguir el ritmo del espectacular aumento del cibercrimen, ya que se provee que este le costará al mundo 6 mil millones de dólares (mdd) anuales.

El presente trabajo de investigación presentará una técnica para la detección de vulnerabilidades en la web, como lo es Banner Grabbing de uso intuitivo y soportado integralmente en herramientas de software. Dicha técnica presenta un enfoque práctico y conceptual para la detección y evaluación de vulnerabilidades en la web. Adicionalmente, se detallará un caso de estudio práctico dentro de la Cooperativa de ahorro y crédito "Riobamba Ltda. Mediante el cual se logra establecer la utilidad y funcionalidad de esta.

1. Requisitos para instalación de la herramienta de simulación GNS3

GNS3 es una plataforma que permite simular topologías de red con imagenes de marcas como Cisco, Juniper y Fortigate entre otros. A continuación, se muestran los requerimientos para la instalación del software GNS3.

1.2 Compatibilidad con Windows

GNS3 es compatible con los siguientes sistemas operativos de Windows:

- Windows 7 SP1 (64 bit).
- Windows 8 (64 bit).
- Windows 10 (64 bit).
- Windows Server 2012 (64 bit).
- Windows Server 2016 (64 bit).

1.3 Requerimientos mínimos

Los siguientes son los requisitos mínimos para un entorno Windows en GNS3:

Ítem	Requerimientos mínimos
Sistema Operativo	Windows 7 (64 bit) o superior
Procesador	2 o más núcleos lógicos
Virtualización	Se requieren extensiones de virtualización. Es posible que deba habilitar esto a través del BIOS de su computadora.
Memoria	4 GB RAM
Espacio en disco	1GB de espacio disponible

Tabla 1: Requerimientos mínimos para GNS 3

2.4 Requerimientos recomendados

Ítem	Requerimientos mínimos
Sistema Operativo	Windows 7 (64 bit) o superior
Procesador	4 o más núcleos lógicos – AMD-V / RVI Series o Intel VT-X / EPT
Virtualización	Se requieren extensiones de virtualización. Es posible que deba habilitar esto a través del BIOS de su computadora.
Memoria	16 GB RAM
Espacio en disco	Disco de Estado Sólido (SDD) 35 GB de espacio disponible

Tabla 2: Requerimientos recomendados para GNS3

2. Descarga de GNS3

Para descargar GNS3 lo puede hacer desde la página oficial https://www.gns3.com/ donde encontrará el boto "Free Download" al dar click se mostrará aparece una pantalla como se muestra en la Fig.

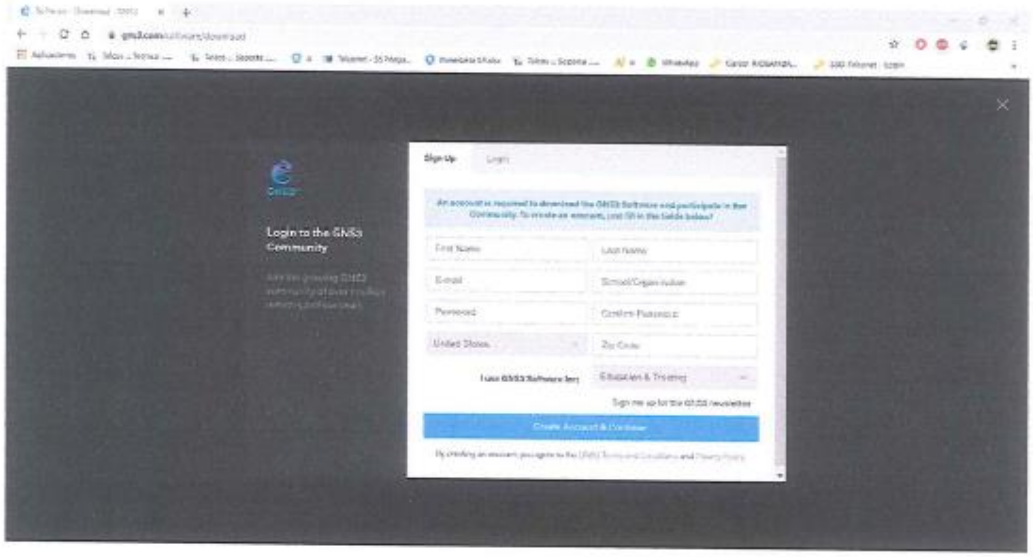


Figura 1: Pantalla de descarga GNS3.

Después es necesario registrarse para poder descargar el simulador una vez que se llene los datos podrá descargar y saldrá la siguiente pantalla que se muestra en la Fig. 2

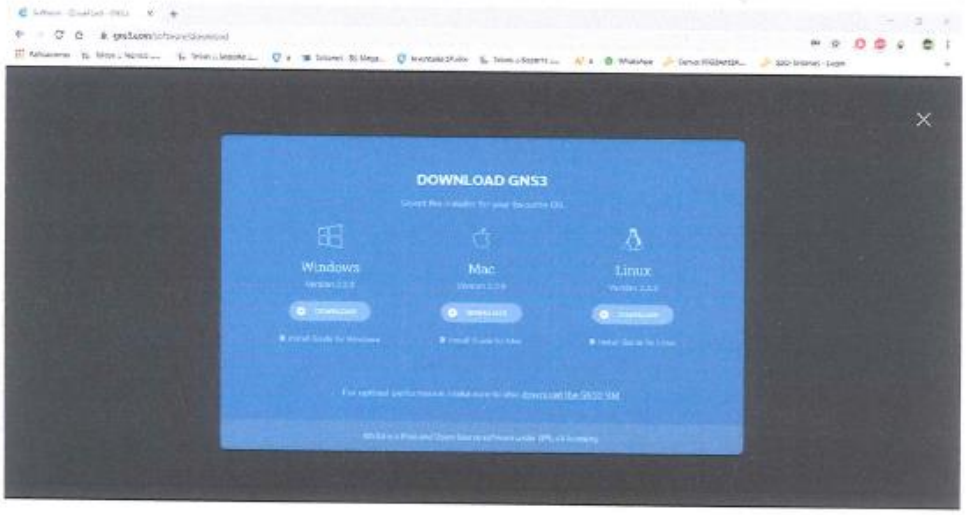


Figura 2: Imagen para descargar GNS3

Como se observa en la Fig. 2 se puede descargar para varias plataformas como son Windows, Linux o IOS. Una vez que de click en "Download" la descarga iniciará automáticamente.

3. Instalación de GNS3

A continuación, se describe el procedimiento de instalación de GNS3 en Windows 10, la ejecución es similar para otras versiones de Windows.

3.1 Inicio de instalación

Una vez finalizada la descarga se debe ejecutar el archivo, luego les pedirá permisos de administrador, le dan Ok y aparecerá la siguiente pantalla según la Figura 3.1, esta hace referencia al acuerdo de licencia para poder ejecutar la instalación GNS3. Dar Click en "Agree".

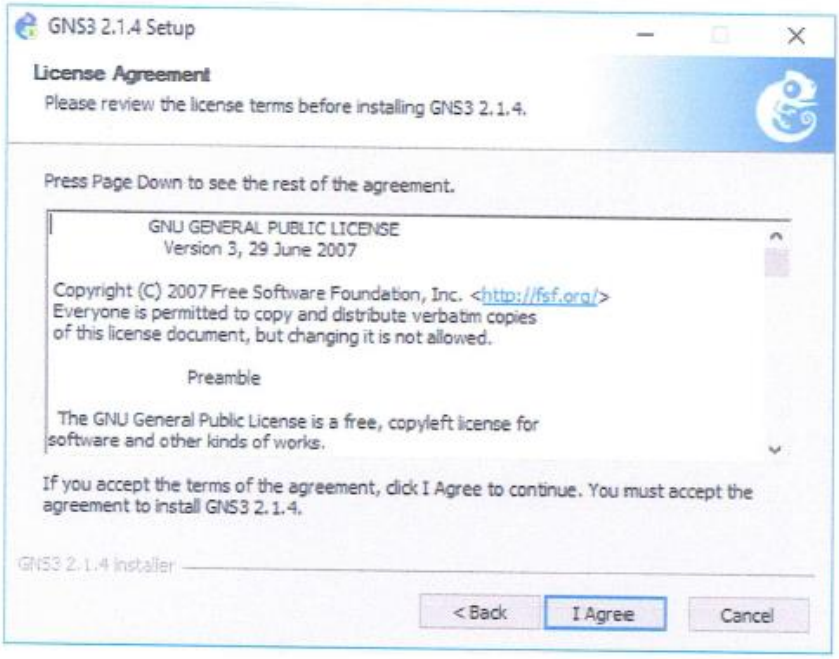


Figura 3: Acuerdos de Licencia para instalar el simulador GNS3

3.2 Selección de componentes para la instalación

A continuación, se solicitará seleccionar los componentes que se instalarán junto con el simulador tal como se muestra en la Figura 4. Considerar la Tabla 3. con relación a los componentes que están incluidos durante la instalación del GNS3, además de la función de cada uno de ellos y la web de sus desarrolladores. Se recomienda seleccionar e instalar los componentes que están en negrita.

Aplicación	Función	Web del Desarrollador
GNS3	Simulador gráfico de red	https://www.gns3.com/
WinPCAP	Permite enviar y capturar paquetes	https://www.winpcap.org/

6

WireShark	Analizador de paquetes	https://www.wireshark.org/
Dynamips	Emulador de router Cisco	https://rednectar.net/tag/dynamips/
QEMU	Ejecuta máquinas virtuales	https://www.qemu.org/
Cpulimit	Limita el uso que hace la CPU en un proceso	https://sourceforge.net/projects/vpcs/
TightVNC Viewer	Control remoto de máquinas virtuales	https://www.tightvnc.com
Solar Winds Response	Analizador de paquetes trabaja con WireShark	https://www.solarwinds.com
Npcap	Sniffer de puertos	https://nmap.org/npcap/
VPCS	Simulador de Terminales (PC)	https://sourceforge.net/projects/vpcs/

Tabla 3: Lista de componentes incluidos en la instalación del GNS3

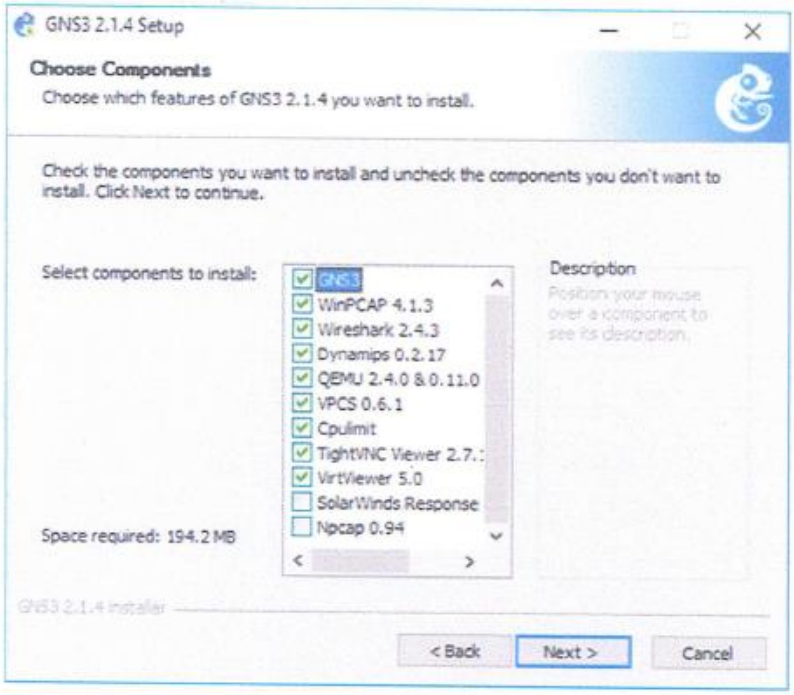


Figura 4: Selección de componentes para la instalación de GNS3

Posteriormente, seleccionar la carpeta donde se instalará la aplicación, en este caso se ha dejado la carpeta por defecto tal como se muestra en la Figura 5.

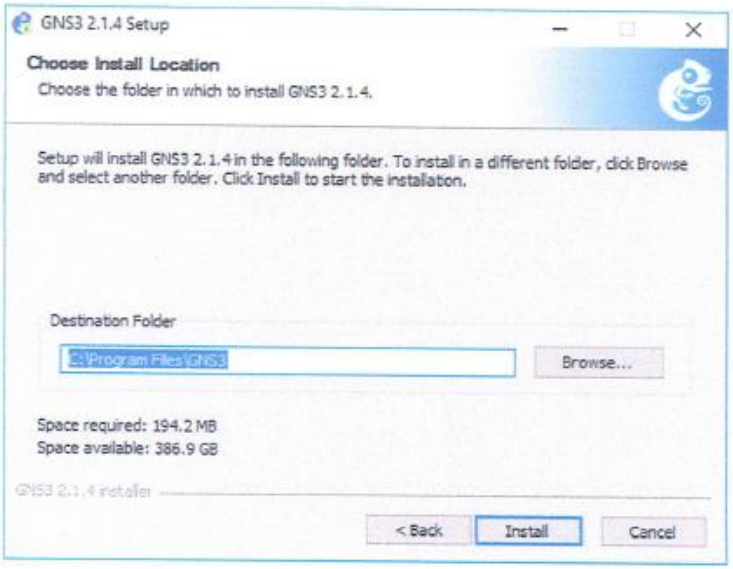


Figura 5: Selección de la carpeta para la instalación

Después se realiza el inicio de la copia de archivos tal como se muestra en la Figura 6. Se instalarán aplicaciones adicionales como el Visual C++, darle los accesos para que pueda ejecutarse la aplicación sin problemas.

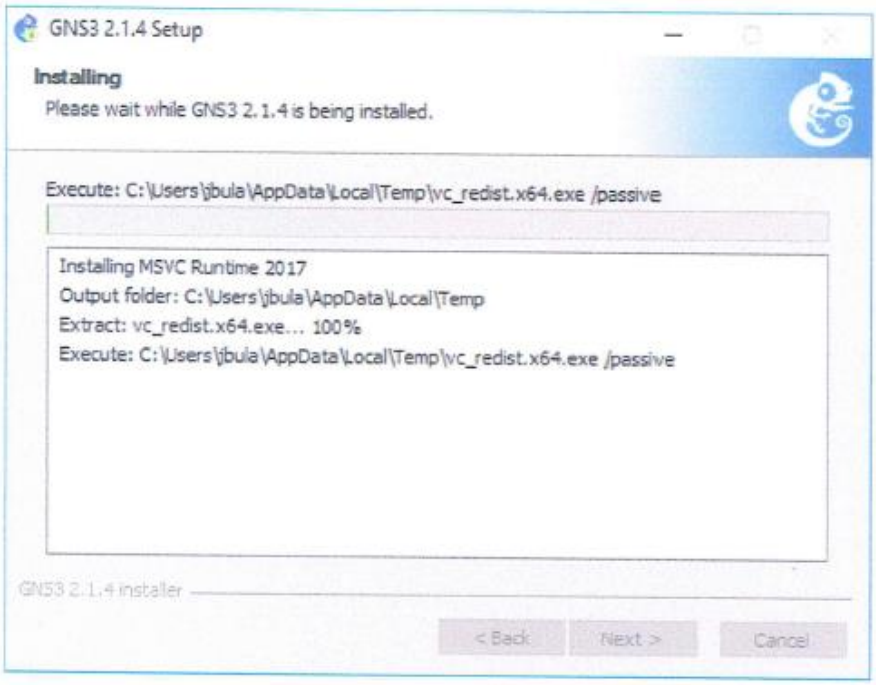


Figura 6: Inicio de instalación en el disco local

En algunos casos se requerirá la conexión a internet para poder descargar aplicaciones como WireShark. (Ver Figura 7).

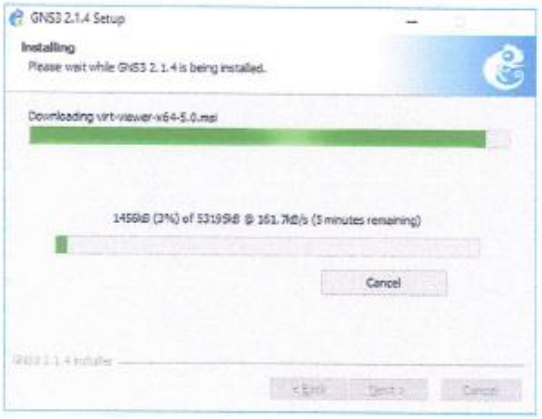


Figura 7: Descarga de aplicaciones de internet

9

Luego se completa la copia de los archivos como se muestra en la Figura 8. click en Next para continuar

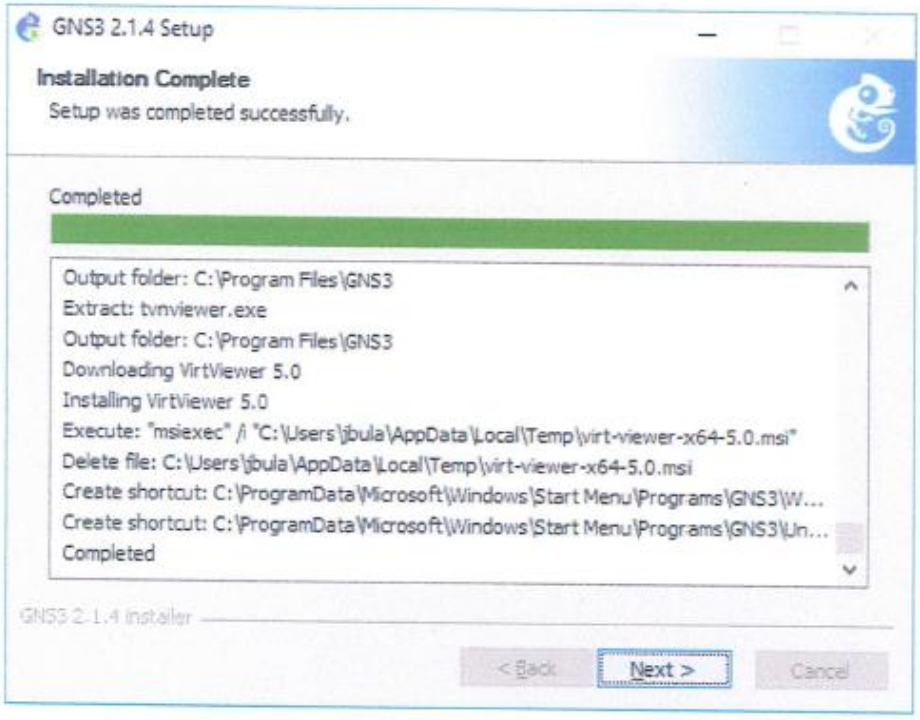


Figura 8: Finalización de copiados de archivos

3.3 Finalización de la instalación de GNS3

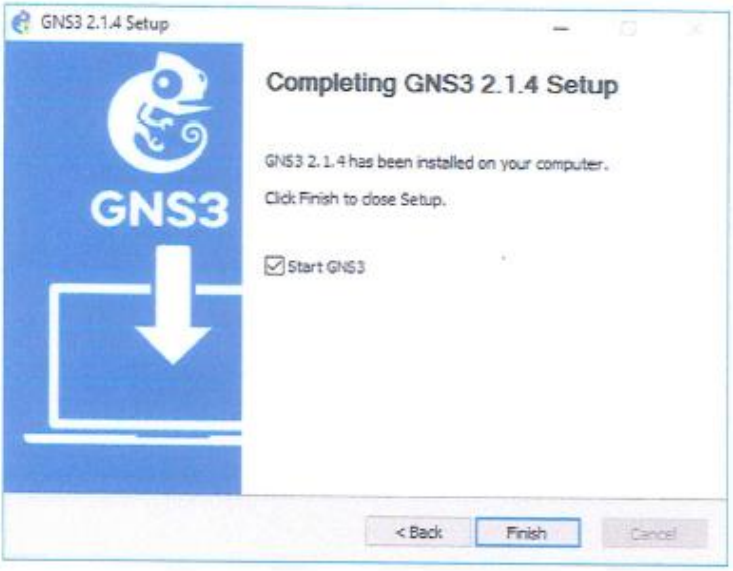


Figura 9: Finalización de la instalación de GNS3

4. Primer inicio de GNS3: Setup Wizard

Luego de la instalación el siguiente paso a seguir es la configuración de la interfaz gráfica de usuario mediante el Setup Wizard, para poder alojar las imagenes IOS, esto se puede realizar mediante una máquina virtual o servidor, la Figura 4.1. muestra la pantalla en el primer inicio de GNS3.

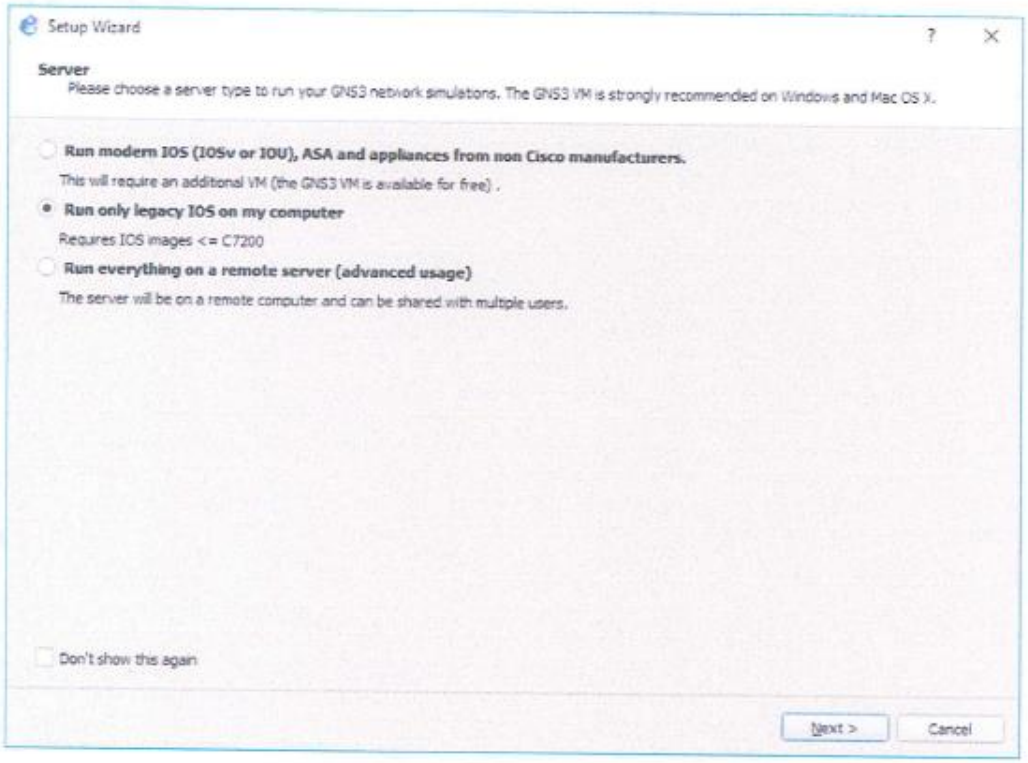


Figura 10: Selección del servidor para la simulación en GNS3.

De acuerdo al menú se tienen tres opciones:

- Run Modern IOS (IOSv or IOU), ASA and appliances from non Cisco manufacturers: Requiriere la configuración de una Máquina Virtual.
- Run only legacy IOS on my computer: La carga de IOS se puede realizar directamente en la plataforma GNS3 mediante servidor local.
- Run everything on a remote server (para usuarios avanzados): se realiza la carga de los dispositivos a través de Servidores remotos.

5. Configuración de Imagenes y Dispositivos

5.1 Iniciar dispositivos IOS modernos (IOSv or IOU) con GNS3 VM

Si se decide usar la máquina virtual GNS3 (recomendado), puede ejecutar la máquina virtual GNS3 localmente en su PC utilizando software de virtualización como VMware Workstation o Virtualbox; o puede ejecutar la máquina virtual GNS3 de forma remota en un servidor utilizando VMware ESXi o incluso en la nube.

Se puede usar GNS3 solo con el servidor local, sin usar la máquina virtual GNS3, esta es una buena manera de comenzar, sin embargo, esta configuración es limitada y no ofrece tantas opciones con respecto al tamaño de topología y los dispositivos admitidos. Si desea crear topologías GNS3 más avanzadas o desea incluir dispositivos como los dispositivos Cisco VIRL (IOSvL2, IOSvL3, ASAv) u otros dispositivos que requieran Qemu, se recomienda la máquina virtual GNS3 VM (y a menudo se requiere).

5.2 Iniciar imagenes IOS antiguas mediante el Servidor Local GNS3

Mediante esta opción se ejecuta las imagenes y dispositivos en la misma PC donde instaló el software todo en uno GNS3. Si, por ejemplo, está utilizando una PC con Windows, tanto la GUI GNS3 como el servidor local GNS3 se están ejecutando como procesos en Windows. Procesos adicionales como Dynamips también se ejecutarán en su PC, en la

siguiente sección se detalla la configuración del servidor local y la carga de imagenes IOS legacy.

6. Configuración del servidor Local GNS3

Mediante el Setup Wizard elegir «Run only legacy IOS on my computer» y dar Next, a continuación, se debe elegir la ubicación donde se encuentra la aplicación «gns3server.exe», además, la IP y el puerto. Se recomienda colocar los siguientes parámetros:

- Server path: Ubicación por defecto del ejecutable gns3server.EXE,
- Host Binding: Colocar IP 127.0.0.1 que es la dirección IP de loopback,
- Port: 3080 TCP

Figura 11: Setup Wizard local server.

En esta sección podemos elegir bajo que host se va ejecutar la VM de GNS3 es recomendable usar la que se muestra en la figura 11. Para que no existan errores en conexiones con dispositivos.

7. Configura una Imagen IOS al Servidor Local GNS3 (Dynamips)

En la pantalla «New appliance template», se podrá agregar una Imagen IOS para GNS3 mediante el servidor Local GNS3 previamente configurado, en este caso es se utilizará la Imagen de un Router Cisco 7200 el cual sirvió para simular el router que da salida a internet a la cooperativa.

Se debe seleccionar "Ad dan IOS router using a real IOS image (supported by Dynamips)", tal como se muestra en la Figura 12

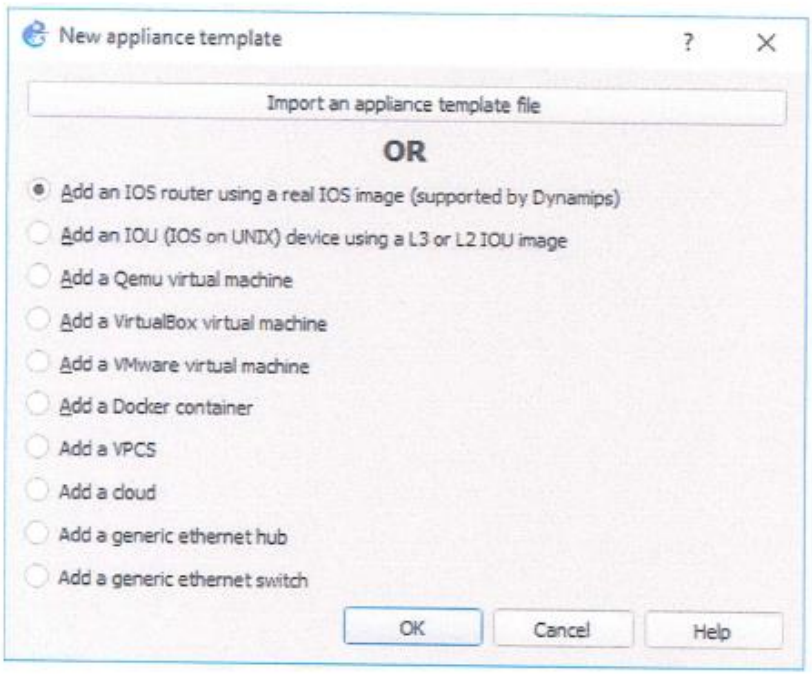


Figura 12: Pantalla que permite agregar un nuevo dispositivo

Luego se debe seleccionar la ubicación del IOS del router Cisco, damos click en "Browse". (Ver Figura 13)

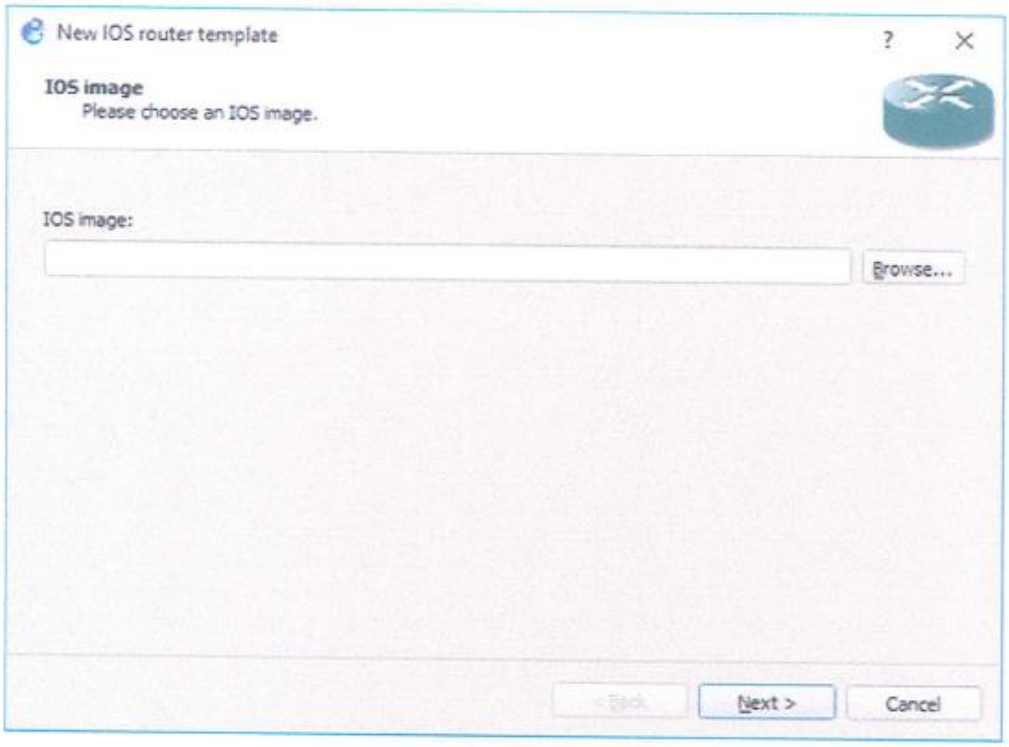


Figura 13: Pantalla para la carga del IOS

Seleccionaremos la ubicación del IOS. (Ver Figura 14)

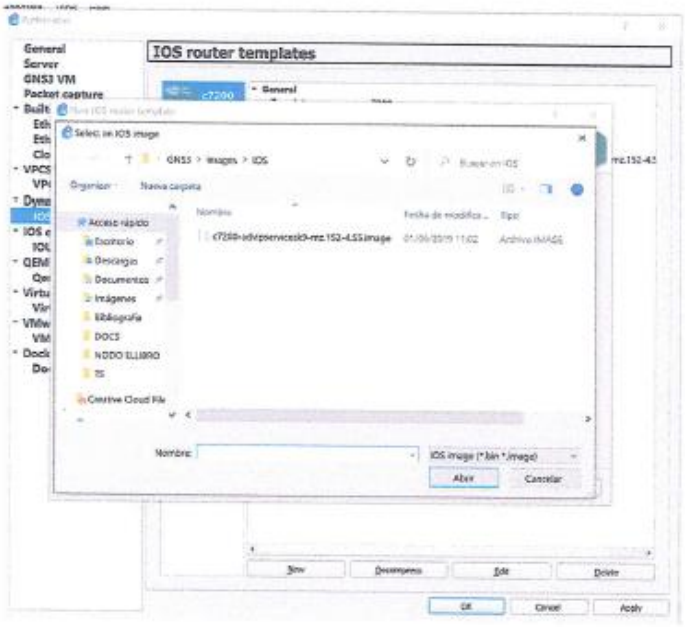


Figura 14: Selección del IOS del router Cisco.

Luego de realizar la selección de la imagen, aparecerá un mensaje que pide si se desea descomprimir la imagen IOS (Ver Figura 15).

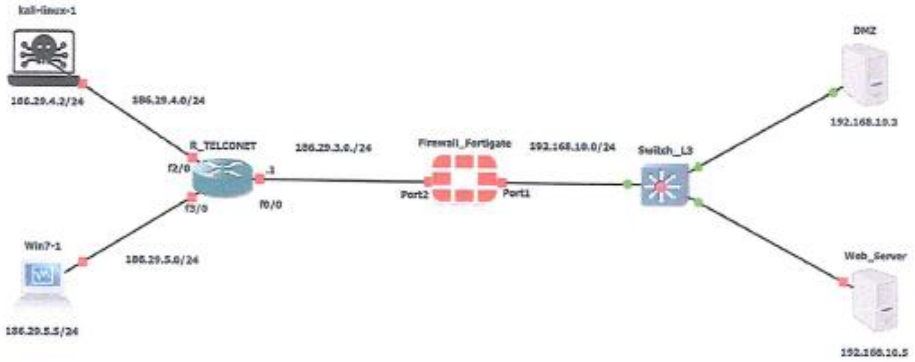
8. Tabla de IPs usadas en la simulación

Tabla 4: Hosts, Interfaces e Ips usadas en la simulación

IP	INTERFACE	HOST
186.29.3.1/24	F0/0	R_TELCONET
186.29.3.2/24	Port1	FortiGate_Firewall
186.29.4.1/24	F2/0	R_TELCONET
186.29.4.2/24	Eth0	Kali Linux
186.29.5.1/24	F3/0	R_TELCONET
186.29.5.2/24	Eth0	Usr_1
192.168.5.1/24	Port2	FortiGate_Firewall
192.168.5.2/24	Port1	FortiWeb_Firewall
192.168.10.1/24	Port2	FortiWeb_Firewall
192.168.10.3/24	Eth0	Servidor DMZ
192.168.10.5/24	Eth0	Servidor WEB

Para la simulación del escenario se usó las ips que se muestran en la tabla 4, se implantaron en base a la configuración mostrada en el esquema de la COAC "Riobamba" Ltda. Se modificaron y adaptaron para ejemplificar de la mejor manera posible en la simulación sin que haya alteraciones en la topología original.

9. Escenario de la COAC con su topología y un ataque externo



10. Configuración Firewall_Fortigate

En primer lugar, verificamos el estado de las interfaces del router Comando: su system interface ver figura 15.

```
FortiGate-VM64-KVM login: admin
Password:
Welcome !

FortiGate-VM64-KVM # sh system interface
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh http fgfm
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set type physical
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set type physical
        set snmp-index 3
    next
    edit "port4"
        set vdom "root"
        set type physical
        set snmp-index 4
    next
    edit "port5"
        set vdom "root"

FortiGate-VM64-KVM #
```

Figura 15: Estado de interfaces Fortigate al iniciar

Posteriormente configuramos las interfaces que van conectadas a la WAN y al switch de nuestro escenario, para el puerto1, ver figura 16.

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port1
FortiGate-VM64-KVM (port1) # set mode static
FortiGate-VM64-KVM (port1) # set ip 192.168.10.1/24
FortiGate-VM64-KVM (port1) # set allowaccess https http ping
FortiGate-VM64-KVM (port1) # end
FortiGate-VM64-KVM #
```

Figura 16: Comandos para configurar puerto 1

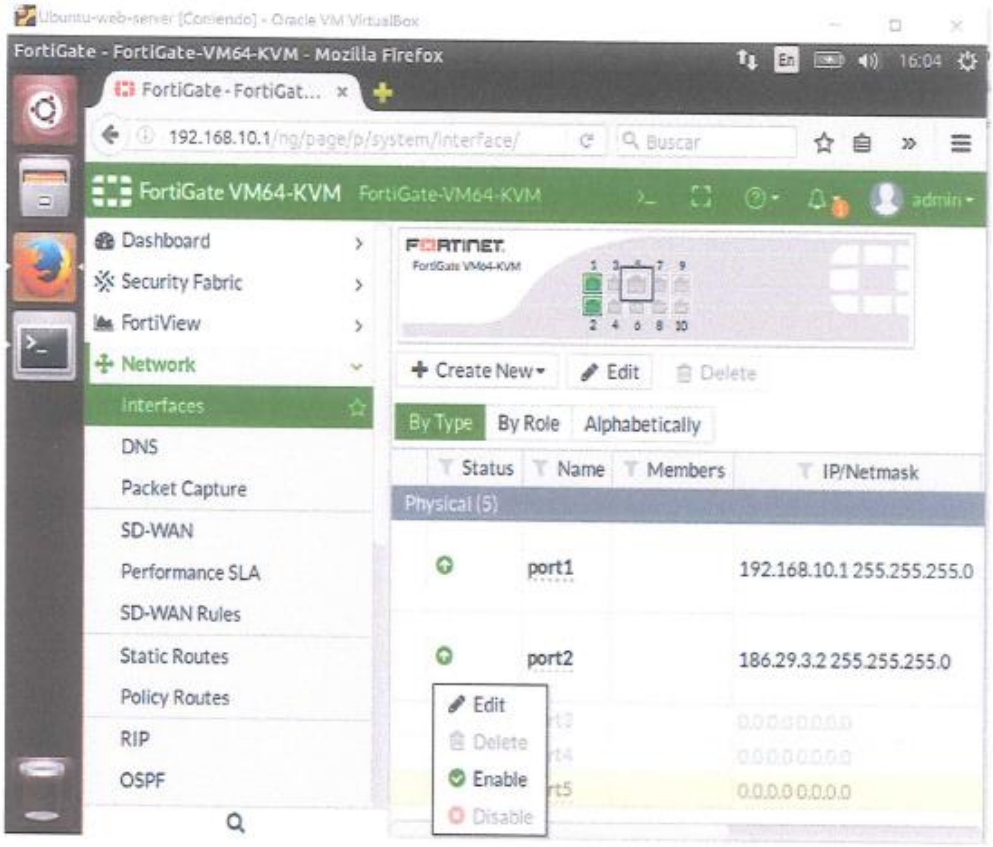
Para el puerto 2:

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port2
FortiGate-VM64-KVM (port2) # set mode static
FortiGate-VM64-KVM (port2) # set ip 186.29.3.2/24
FortiGate-VM64-KVM (port2) # set allowaccess https http ping
FortiGate-VM64-KVM (port2) # end
FortiGate-VM64-KVM #
```

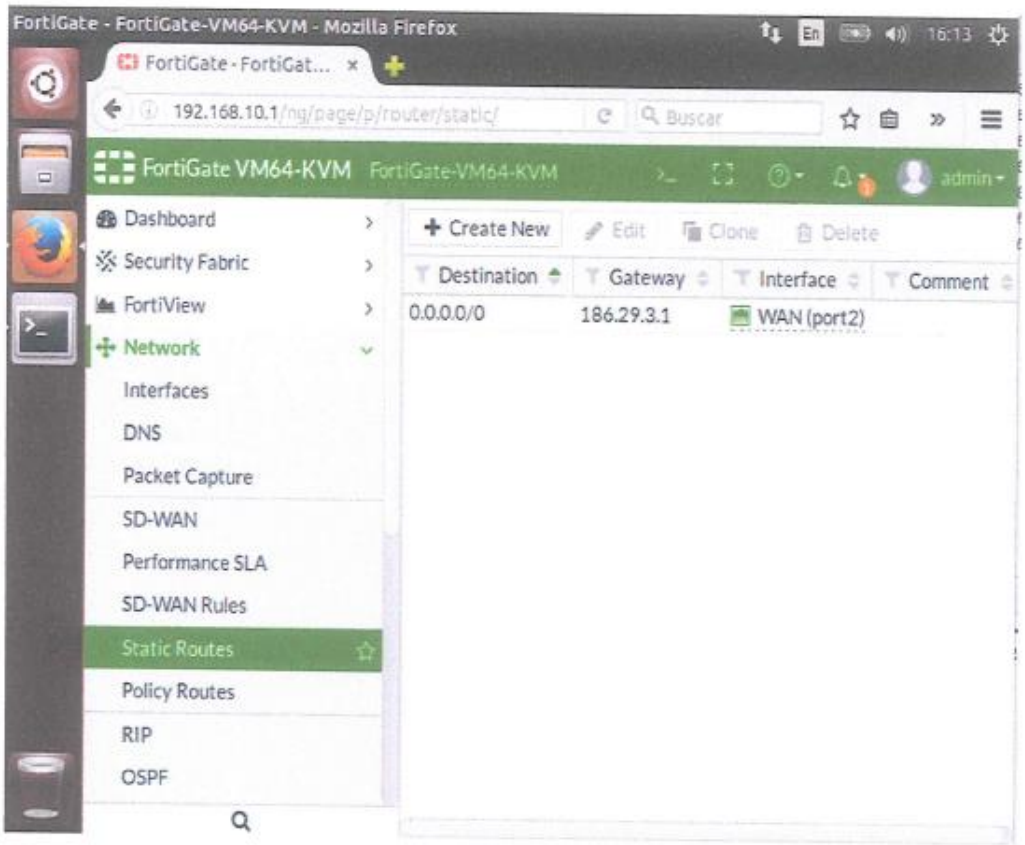
Figura 17: Comandos para configurar puerto 2

Se configuran los puertos con ip estáticas de acuerdo al escenario planteado una vez hecho esto tendremos acceso a configurar el router mediante la interfaz gráfica.

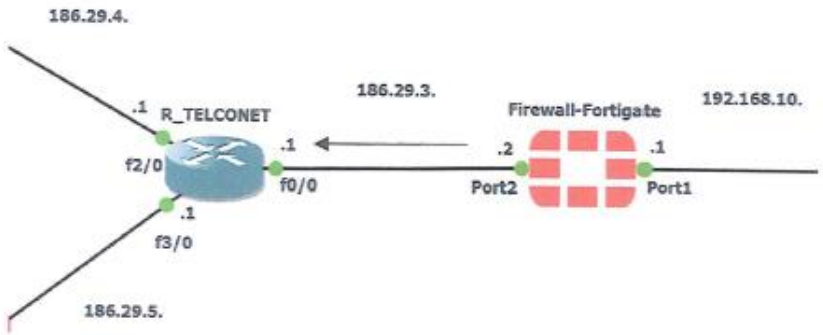
Dentro de la interfaz configuramos los puertos, debemos desactivar administrativamente los que no se usarán por seguridad:



Posteriormente configuramos una ruta estática para que reconozca la red que viene de la WAN en nuestro escenario:



Por cuestiones investigativas en la IP destino dejamos 0.0.0.0 para que puedan acceder todas las ips a nuestro servidor web en el Gateway configuramos el siguiente salto de red como se puede ver en el escenario planteado.



20

Como siguiente paso debemos configurar una política de IPv4 para que haya comunicación dentro del escenario planteado:

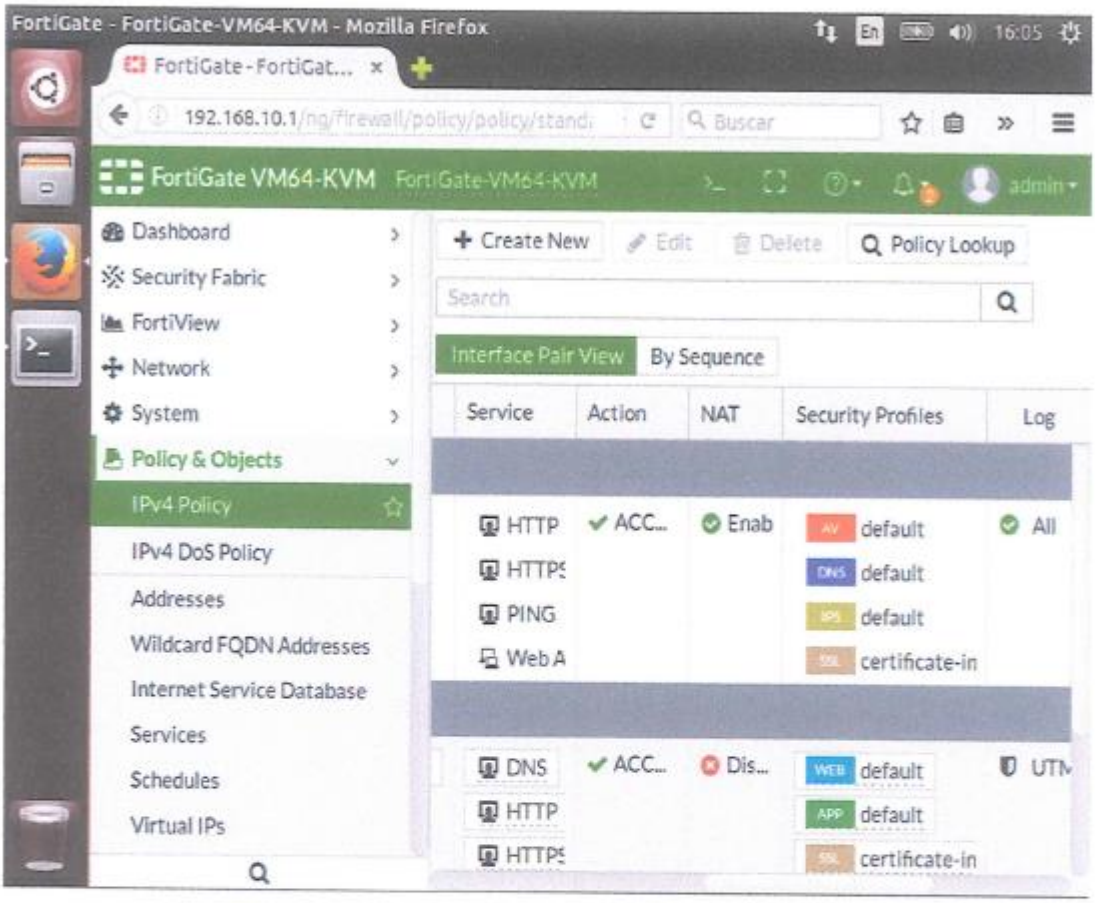


Figura 18: Políticas IPv4 para el Firewall Fortigate

Como se muestra en la figura 18, la configuración de las políticas para IPv4 es importante para que el router pueda comunicarse con las interfaces que entran a la LAN y sales a la WAN es decir a internet. Además, en este apartado aplicamos ciertos filtros para mayor seguridad en la red.

Una vez realizada esta configuración está listo el primer router del escenario virtual.

11. Configuración de Firewall_Fortiweb

En el siguiente paso se procede a configurar el router que funciona como firewall web

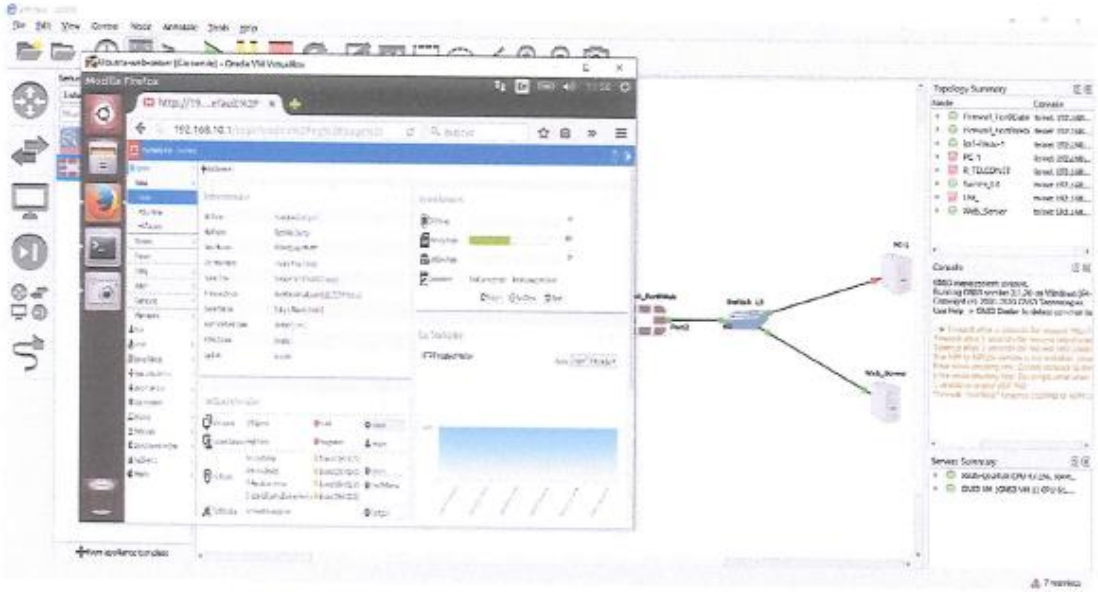


Figura 19: Pantalla de inicio firewall FortiWeb

La figura 19, muestra la pantalla principal del FortiWeb usado para la simulación este router tiene 5 interfaces Gigabit Ethernet, 1024 MB de RAM y 1 vCPU. Este firewall cuenta con herramientas de protección completa y especializada a todos los niveles para las aplicaciones y servicios Web. Algunas de las características de seguridad que ofrece son:

- Cross-Site Scripting (XSS).
- Cross-Site Request Forgery (CSRF).
- Insecure Cryptographic Storage.
- Failure to Restrict URL Access.