ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

IMPLEMENTACIÓN Y EVALUACIÓN DE UN SISTEMA DE SEGURIDAD ANTI PHISHING PARA PROTECCIÓN DE LA INFORMACIÓN UTILIZANDO UN FIREWALL EN PROCEDIMIENTOS ACADÉMICOS EN LÍNEA PARA EL INSTITUTO SUPERIOR TECNOLÓGICO RIOBAMBA

MARCO VINICIO ESTRADA VELASCO

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD EN TELEMÁTICA

Riobamba – Ecuador

Mayo 2022

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado: Implementación y evaluación de un sistema de seguridad anti-phishing para protección de la información utilizando un Firewall en procedimientos académicos en línea para el Instituto Superior Tecnológico Riobamba, de responsabilidad del señor Marco Vinicio Estrada Velasco, ha sido prolijamente revisada y se autoriza su presentación.

Tribunal:

Ing. Luis Eduardo Hidalgo Almeida, Ph. D.	LUIS EDUARDO HIDALGO ALMEIDA **PRESIDENTE**
Ing. Cristian Geovanny Merino Sánchez, Mag.	CRISTIAN GEOVANNY MERINO SANCHEZ Firmado digitalmente por CRISTIAN GEOVANNY MERINO SANCHEZ **DIRECTOR**
Ing. Oswaldo Geovanny Martínez Guashima, M. Sc.	OSWALDO GEOVANNY MARTINEZ GUASHIMA Firmado digitalmente por OSWALDO GEOVANNY MARTINEZ GUASHIMA **MIEMBRO DEL TRIBUNAL**
Ing. Joffre Stalin Monar Monar, Mag.	JOFFRE STALIN MONAR MONAR **MIEMBRO DEL TRIBUNAL**

Riobamba, mayo 2022

DERECHOS INTELECTUALES

Yo, Marco Vinicio Estrada Velasco, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo** y que el patrimonio intelectual generado por la misma pertenece a la Escuela Superior Politécnica de Chimborazo.

_____

Marco Vinicio Estrada Velasco
0603570672

DECLARACIÓN DE AUTENCIDAD

Yo, Marco Vinicio Estrada Velasco, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

_____

MARCO VINICIO ESTRADA VELASCO
C.C: 0603570672

DEDICATORIA

A mis padres, hermanas, sobrinas y amigos, que me ayudaron y me motivaron a terminar este proceso. Muchas gracias

Marco Estrada.

AGRADECIMIENTO

A la Escuela Superior Politécnica de Chimborazo por permitirme seguir formándome ahora con un título de cuarto nivel, a sus autoridades y docentes que nos impartieron sus cátedras, también a mi director de maestría por confiar en mí y no dejarme derrumbar.

A mis padres, hermanas y sobrinas por siempre ser el pilar fundamental de mi vida.

Marco Estrada

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo fue implementar y evaluar un sistema de seguridad anti-phishing para dar una protección de la información del Instituto Superior Tecnológico Riobamba, implementando las normas ISO 27001. Se llevó a cabo pruebas en dicha plataforma informática para detectar vulnerabilidades, utilizando el sistema de seguridad basado en la norma ISO 27001 para su prevención. La detección de vulnerabilidades se basó en 5 de los riesgos de seguridad encontrados mediante el Open Source, utilizando como herramientas de escaneo y explotación a Nessus, Vega, BurpSuite y Zenmap, Kali Linux (metasploit), lo que facilitó identificar fallas de seguridad como: inyección de código malicioso, pérdida de autenticación, exposición de datos sensibles, pérdida de control de acceso, control de seguridad incorrecta, uso de componentes con vulnerabilidades conocidas y registro y monitoreo insuficientes; se identificó que la plataforma informática presentó todas las 8 vulnerabilidades establecidas. Se concluyó que la plataforma en un 100% pudo verse afectada, por ésta razón se diseñó el plan de seguridad con directrices de mejora acorde a las vulnerabilidades encontradas, mismo que fue implementado por un periodo de prueba de dos meses, dando como resultado una mejora significativa en el nivel de seguridad, reduciendo de 7 a 2 las vulnerabilidades existentes en dicha plataforma, y la implementación del plan de seguridad permitió una mejora del 75% de la plataforma informática de la institución. Se recomienda seguir implementando políticas de seguridad para generar una cultura preventiva en los funcionarios y seguir evitando situaciones de riesgo.

Palabras clave: <SEGURIDAD TELEMÁTICA >, <FIREWALL>, <OPENSOURCE>, <VULNERBILIDADES >, <PHISHING >, <ANTI PISHING >

SUMMARY

The research objective was to implement and evaluate an anti-phishing security system to give protection to data at The Institute of Higher Technology Riobamba, implementing the ISO norms 27001. Testing was carried out on the computing platform in order to detect vulnerabilities, using a security system based on ISO 27001 norm for its prevention. The detection of vulnerabilities was based on 5 security risks found through Open Source, using scanning and exploitation tools such as Nessus, Vega, BurpSuite and Zenmap, Kali Linux (metasploit), which allowed the identification of security failures like: malicious code injection, authentication loss, sensitive data exposure, loss of access control, incorrect security control, use of components with known vulnerabilities and insufficient register and monitoring. Moreover, it was identified that the computing platform registered all 8 established vulnerabilities. It was concluded that the platform could have been 100% affected, therefore a security plan including best practices and guidance was designed, taking into account the vulnerabilities found, such plan was implemented and tested for a trial period of one to two months, resulting in a significant improvement in the level of security, reducing from 7 to 2 the number of vulnerabilities of the platform. The implementation of the security plan allowed a 75% improvement of the institution's platform. The continuity of the implementation of security policies is recommended, in order to generate a preventive culture within the staff members and prevent risky situations in the future.

Keywords: <<TELEMATICS SECURITY>>, <<FIREWALL>>, <<OPENSOURCE>>,<<VULNERABILITIES>>, <<PHISHING>>, <<ANTI PHISHING>

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Antecedentes

La tecnología ha ido evolucionando con el pasar de los tiempos y las entidades que manejan este recurso han facilitado el uso de datos para varias operaciones en cuanto a los servicios de internet. Las empresas envían la información a través de los servicios web, que al encontrarse en una libre disposición tienen un fácil acceso por personas externas a la entidad.

Las plataformas informáticas son herramientas conformadas por hardware y software que dan a las empresas servicios del sistema informático tradicional como: accesibilidad, disponibilidad e integridad mediante diferentes conexiones web.

La evolución de varias plataformas como de aplicaciones web y móviles han hecho que también los ciberataques sean capaces de penetrar varias seguridades de diferentes entidades públicas y privadas que están colgadas en la web. Para esto se debe brindar la seguridad, otorgando la protección de la información; evitando de esta manera problemas fraudulentos ocasionados por terceras personas al no conocer sobre el tema.

El Instituto Superior Tecnológico Riobamba al ser una institución de educación pública maneja información propia y de otros establecimientos, es por esto que, al no resguardar su información de manera adecuada, estos recursos han presenciado el intento de ser vulnerados debido al libre acceso por estudiantes, docentes y público en general.

Con este trabajo de investigación se propone diseñar e implementar un modelo de seguridad evitando la fuga de información y el acceso no autorizado de personas externas a la institución ya que la importancia de los datos en la plataforma digital académica son muy delicados y propensos a ser modificados.

1.2 Planteamiento del problema

1.2.1 Situación problemática

Actualmente el desarrollo continuo de la tecnología, su evolución y las nuevas formas de comunicarnos en el mundo por el avance de las redes hace que la web se vea vulnerada por el

mal uso de la información por el incremento de ciberataques al perder el control de su seguridad, ocasionando pérdidas económicas y daños personales.

Por tanto, mantener resguardada la información es de un preciado valor para las compañías, empresas, instituciones de educación y usuarios de páginas web.

El Firewall instalado y conectado directamente con los servidores protege de las amenazas que provienen de la red pública (internet), aceptando o negando requerimientos de los usuarios programando reglas establecidas para el correcto funcionamiento de los sistemas académicos en línea del Instituto Superior Tecnológico Riobamba.

1.2.2 Formulación del problema

¿La implementación de un sistema de seguridad anti-phishing mediante la protección firewall permite proteger la información en un sistema académico en línea?

1.2.3 Sistematización del problema

a) ¿Cuáles son las características de los sistemas anti-phishing?
b) ¿Qué herramientas son las más adecuadas para el diseño e implementación de un sistema anti-phishing?
c) ¿Qué tipos de ataques causan mayor inseguridad a un sistema académico?
d) ¿Cuáles son los parámetros de evaluación para proteger el sistema en línea?

1.3 Justificación de la investigación

La vulnerabilidad de la información se ve afectada por terceros que roban, dañan, amenazan y utilizan mal los datos de las entidades. Es por esto que la seguridad informática nace con el objetivo de cuidar y evitar eventos no planeados.

El Instituto Superior Tecnológico Riobamba brinda un servicio de educación a la ciudadanía, que facilita el acceso de internet permitiendo visualizar notas, descargar información, subir deberes entre otros; que representan amenazas debido que no hay una correcta seguridad y perjudica su desempeño.

Al evaluar e implementar un software en la institución, el personal administrativo evitará intrusiones no adecuadas por extraños que deseen perjudicar la misma y así evitar vulnerabilidades de la información.

De esta manera un sistema de seguridad anti-phishing ayuda a prevenir la exposición de situaciones no controladas y asegurar el beneficio de estudiantes y el personal de la entidad que son los beneficiarios directos, adquiriendo una protección de su información.

Para lograr un adecuado manejo de la información y los datos existentes se requerirán acciones como un proceso lógico, sistemático, documentado que facilite la seguridad de la información. Así mediante la implementación del Firewall Open- Source garantiza que los usuarios corporativos puedan manejar las funciones que son esenciales de la red.

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Implementar y evaluar un sistema de seguridad anti phishing para protección de la información utilizando un firewall en procedimientos académicos en línea para el Instituto Superior Tecnológico Riobamba.

1.4.2 Objetivos específicos

a) Determinar las vulnerabilidades existentes en los sistemas académicos en línea del Instituto Superior Tecnológico Riobamba mediante la norma ISO: 27001 de seguridad de la información.
b) Elaborar un escenario de prueba para comprobar la seguridad y acceso a la información de los usuarios que ingresan a los servicios en línea que ofrece el Instituto Superior Tecnológico Riobamba.
c) Diseñar un sistema de seguridad anti-phishing utilizando firewall en los procedimientos académicos en línea, logrando proteger la información sensible.
d) Evaluar los resultados del sistema de seguridad anti-phishing y comparar con el diseño actual de red del Instituto Superior Tecnológico Riobamba.

1.5 Planteamiento de la hipótesis

La implementación de un sistema de seguridad anti-phishing con firewall mejorará la integridad y confidencialidad de la información en los sistemas en línea para el Instituto Superior Tecnológico Riobamba.

CAPÍTULO II

2 MARCO DE REFERENCIA

2.1 Antecedentes del problema

El phishing ha perjudicado a muchas entidades ya que se ha convertido en un ataque preferido por los piratas informáticos vulnerando bases de datos de las instituciones.
En el año 2016 se implementó un supervisor Antispam Email Gateway en la infraestructura de comunicación del Gobierno Autónomo Descentralizado de la Provincia de Chimborazo, protegiendo la información en su sistema por la efectividad del control del spam y la calidad de este en su función. (Corozo, 2016)

En el 2018 Valente propone una metodología para detectar la vulneración y mejorar la seguridad en la red de datos, donde realizó fases metodológicas investigando el aumento de la seguridad, personal, física, lógica y legal determinando que puede aplicarse a cualquier medio considerando una exhaustiva fase de evaluación de riesgos. (Valente, 2018)

Según estudios realizados se evidenció que los usuarios de las entidades son vulnerables a ataques en la red debido a que no se presta atención a la seguridad de los dispositivos y que puedan fácilmente acceder usuarios no autorizados. Así en el año 2019 se realizó pruebas aplicando la metodología pentesting en cuatro fases utilizando herramienta Yersinia donde finalmente se elaboraron políticas de seguridad logrando mitigar la vulnerabilidad en los equipos y obteniendo un resultado favorable. (Pilamunga, 2019)

En un estudio realizado en el año 2021 se plantea una propuesta de un plan de seguridad para prevenir las vulnerabilidades en la plataforma informática del Cuerpo de bomberos en el Gobierno Autónomo Descentralizado Municipal de Santo Domingo donde se evidenció las mayores vulnerabilidades de la información que ocurren al inicio de sesión, envío de información confidencial y el fácil acceso a usuarios no autorizados. Una vez que se implementa el plan de seguridad se determinó que la exposición de la información llega a ser en menor cantidad ya que los datos no se encuentran tan vulnerados. (Pinango, 2021)

2.2 Bases teóricas

2.2.1 Firewall o cortafuegos funcionamiento

Un Firewall funciona como un embudo por el que pasan los datos que circulan por una LAN, manteniendo en control a los usuarios restringidos o malintencionados tales como hackers, crackers, vándalos y espías. Un Firewall también sirve para alertar al Administrador de un posible ataque o fuga de seguridad, por medio de correos electrónicos, mensajes de texto por celular o un mensaje por un Beeper las cuales son las maneras más frecuentes de dar alarma. Todo esto brinda la oportunidad de actuar a tiempo para poder terminar, cerrar o aislar el posible ataque, fuga o problema, y de ser necesario apagar y reiniciar toda la red. Como parte de la gestión de seguridad en la red, después de este tipo de eventos es recomendable realizar un informe y encontrar las causas del suceso para así poder hallar una solución y evitar que pueda suceder de nuevo ante las "narices del administrador". Adicionalmente, el Firewall brinda una mayor seguridad en la red interna de la institución, protegiéndola contra amenazas informáticas y proporcionando control al administrador de la red para supervisar la actividad de los usuarios en ésta y así evitar que ellos, por ejemplo, realicen descargas ilegales hacia o desde el Internet. Esta protección brinda seguridad a la institución para evitar problemas legales por infracción a los derechos de autor u otros. (Jiménez, 2014)

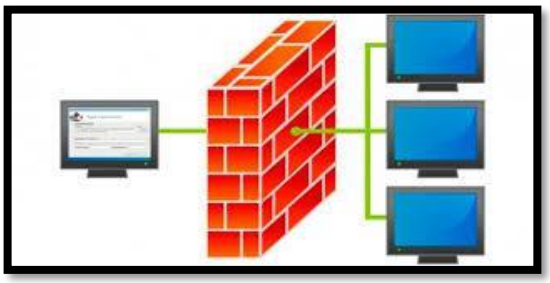


Figura1-2: Firewall cortafuegos

Fuente: (De Luz, 2021)

2.2.2 Beneficios y limitaciones de un Firewall

Un Firewall es la simplificación del trabajo para el Administrador de la red, ya que permite gestionar un solo equipo y así proteger al resto sin modificar los cientos de posibles computadores que existen en la red, evitando que se reduzca su tiempo. "Implementación de un Servidor/Firewall GNU/Linux en un entorno escolar Así se pueden examinar a fondo los

archivos y conocer las páginas a las que se han ingresado, qué procesos o programas han entrado a Internet, y saber qué usuario ha hecho qué. Es muy útil porque para aplicar sanciones se tienen pruebas sólidas de lo sucedido. Cabe aclarar que si uno de los usuarios está empeñado en acceder a la red privada de la institución o quiere filtrar información este lo puede lograr si se empeña en hacerlo. La misión de un Firewall es hacer más dura esta labor, más no imposible; la seguridad total no existe. Por más segura que pueda ser una red siempre habrá un eslabón débil en esta cadena: el factor humano. A una persona se le puede engañar para que revele contraseñas, ayude a descubrir agujeros de seguridad o reemplace al atacante. Esto puede ocurrir de diversas formas, pero un Firewall ayuda a prevenir la mayoría de estas: filtrando el SPAM, denegando el acceso a la red a programas no permitidos y vigilando lo que el usuario lee en la Web. Un Firewall no puede hacer todo esto por sí solo, para ello necesita la ayuda de otro de los componentes que conforman la red: la estación de trabajo que comúnmente se usa con Windows. Es común encontrarse con estaciones que no están correctamente configuradas y que pueden permitir la fuga de información, la ejecución de un programa no permitido, o una infección de Malware." (Analuisa, 2009)

¿Por qué utilizar una red firewall?

El propósito de una red firewall es dar una seguridad a nuestros equipos conectados en red evitando así que las computadoras sean vulnerables a los virus informáticos.

Al configurarse adecuadamente funciona como un escudo para nuestro ordenador, analizando entrada y salida de datos. Hay que considerar que el término open source alcanza un acceso código fuente.

Los programas open source colaboran a usuarios que configuren las funciones de su red. Una de las características que facilitan un escudo de protección son: firewall, antivirus, servicios antispam y filtros web.

Características:

a) Funciones de routing y firewall avanzadas
b) NAT (Traducción de Direcciones de Red).
c) Balanceador de carga.
d) Dispone de cliente/servidor VPN con IPsec y OpenVPN
e) Monitorización avanzada de la actividad de red mediante logs y gráficos.
f) Servidor DNS

g) Sistemas IDS/IPS con Snort o Suricata protección de la red.
h) DNS dinámico y portales cautivos.
i) Servicios DHCP y DCHP Relay.
j) Posibilidad de instalación de software adicional para tener más servicios disponibles.

(Bonilla, 2016)

Tipos de Firewall

A Nivel de Red

Toman decisiones según su dirección de procedencia, dirección de destino y puerto de cada uno de los paquetes IP. Los actuales cortafuegos de nivel de red permiten mayor complejidad a la hora de decidir; mantienen información interna acerca del estado de las conexiones que pasan por él, los contenidos de algunos datos. Estos sistemas, como es lógico, han de tener una dirección IP válida. Este tipo de firewall ocupa la capa 3 del modelo OSI (Open System Interconnection) que es la Interconexión de sistemas abiertos, la cual se encarga de la transmisión de paquetes y de encaminarse cada uno en la dirección adecuada, pero puede tener pérdida o errores de los datagramas.

A Nivel de Aplicación

Generalmente son Host con servidores Proxy, que no permiten el tráfico directamente entre dos redes, sino que realizan un seguimiento detallado del paso de datos por él. Este tipo de firewall pueden ser usados como traductores de red, según pasa el requerimiento y el direccionamiento de paquetes de información.

Beneficios de los firewalls

Permiten al administrador de la red definir un filtro, manteniendo al margen a los usuarios no autorizados (hackers, crackers, espías), protegiendo potencialmente la entrada o salida de usuarios que acceden a la red y a los dispositivos que están conectados.

Un firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generará una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el tránsito de los datos. Debido a todo lo anterior, “un firewall” más “actualizaciones periódicas del software” más “responsabilidad” hace que un conjunto haga una gran defensa para conexiones en red o individuales.

Cómo funciona un sistema firewall

Un sistema firewall contiene un conjunto de reglas predeterminadas que le permiten al sistema.

a) Autorizar la conexión (permitir).

b) Bloquear la conexión (denegar).

c) Rechazar el pedido de conexión sin informar al que lo envió (negar).

2.2.3 Inconvenientes de un firewall

Normalmente el firewall detecta qué programas quieren comunicarse a través de un determinado puerto y lo que hace es preguntar al usuario si desea permitirlo. De esto deducimos dos inconvenientes del firewall:

- El usuario tiene la responsabilidad de decidir cuidadosamente que programas permite comunicarse y cuáles no. Esto requiere un pequeño mantenimiento y esfuerzo del usuario.
- Cuando se permite a un programa utilizar un puerto, recae la responsabilidad de evitar cualquier ataque de seguridad a través de los permisos del firewall.

2.2.4 Bases para el diseño de un firewall

Cuando se diseña un firewall de Internet, se tiene que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

- La política interna propia de la organización para la seguridad total.
- El aspecto económico al momento de implementar un firewall dentro de una empresa.

Políticas de un firewall

Las actitudes del sistema firewall describen la filosofía fundamental de la seguridad de la organización. Estas dos posturas son opuestas de la política de un firewall de Internet considerando que:

"No todo lo específicamente prohibido está permitido" La primera postura asume que un firewall puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso. La segunda asume que el firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitará ser aislado. Esta propuesta crea ambientes más flexibles al disponer más servicios para los usuarios de la comunidad, además, el administrador de la red está en capacidad de incrementar la seguridad en

el sistema. Como del firewall, el cual inmediatamente después de ejecutar una aplicación nos permite la opción de autorizar, denegar o bloquear cierta ejecución.

2.3 Amenaza

Una amenaza ha sido definida como un tipo de acción que logra ocasionar un daño sobre los elementos del sistema, infringiendo sobre todo en la seguridad de los sistemas informáticos. Los nuevos avances tecnológicos nos han otorgado muchos beneficios y comodidades, pero también ha surgido muchas novedades respecto a incidentes de ciberseguridad que cada día son más frecuentes, debido que la confidencialidad de la información muchas veces se encuentra en riesgo y esto surge por la falta de información sobre la relación entre el mundo físico y el virtual. (RAE, 2020)

2.4 Tipos de intrusos informáticos

- ✓ Hackers: Se refiere a aquellas personas que se prestan a programar mediante su conocimiento. Ellos logran acceder a la información confidencial de cualquier entidad o institución.
- ✓ Sniffers: Individuos dedicados a dar seguimiento y descifrar mensajes que presentan ordenadores como el internet.
- ✓ Phreakers: Personas que tienen la característica de sabotear sistemas telefónicos; ellos llaman gratuitamente perjudicando anomalías en las líneas de teléfono.
- ✓ Spammers: un conjunto de individuos que emiten correos e-mails colapsando el buzón del correo de los usuarios transformándolos en virus informáticos.
- ✓ Piratas informáticos: Individuos encargados de replicar programas y contenido digital, perjudicando la autoría intelectual y haciendo de este un negocio como por ejemplo películas, música.
- ✓ Creadores de virus: Personas que diseñan herramientas o programas consiguiendo que se expandan de manera exponencial, y obtienen acceso a números de cuentas bancarias.

2.5 Hacking ético

Se ha definido como el Hacking ético que se otorga a aquellas personas que de manera profesional realizan visualizar la información de manera ética. Estos individuos son contratados para ingresar a los sistemas e identificar y solucionar las vulnerabilidades que suscitan por hackers maliciosos. A estos profesionales se los llama hacker de sombrero blanco y así diferenciarlos de piratas informáticos criminales llamado hackers de sombrero negro.

2.6 Tipos de hackers

En cuanto a los piratas informáticos se los ha clasificado en tres tipos: piratas informáticos sombrero negro, sombrero gris y sombrero blanco.

Sombrero negro: Son aquellos individuos que piratean la información por medio de recompensas o por ganancias financieras.

Sombrero blanco: Son aquellos individuos que tratan de mejorar y solucionar vulnerabilidades de los sistemas, utilizando un hacking ético y notifican a la víctima para que pueda dar un arreglo antes de recibir un ciberataque.

Sombreros grises: Son individuos ubicados entre ambos campos, con operaciones más cuestionables como hackear grupos que se oponen o lanzar protestas hacktivistas. La manera en que estos operan a los atacantes da una visualización de cómo prevenir los ataques.

El hacking ético se define como una destreza que se tiene en las redes para manejar sistemas informáticos que facilita a las organizaciones a poner a prueba la seguridad de su institución con tal de identificar las posibles debilidades y vulnerabilidades.

A partir del hacking ético se identifica como lidiar con piratas informáticos y se concede el permiso de administradores que otorgan permisos para la realización de pruebas.

Para dar seguimiento al hacking ético se considera los siguientes puntos:

- Contrato de acuerdo firmado
- Acuerdo de confidencialidad de la información
- Realizar pruebas sin sobrepasar límites
- Analizar resultados obtenidos de las pruebas
- Presentar hallazgos al cliente.

Fases del hacking ético

1. **Reconocimiento:** En esta fase inicial es donde se investiga y junta la información y se planifican puntos débiles.
2. **Escaneo de la red:** Información específica de aquellos sistemas operativos, puertos y otros.
3. **Ganar acceso a los sistemas:** En esta fase las técnicas a usarse son el crackeo de contraseñas.
4. **Escalado de privilegios/mantener el acceso:** Acceso al sistema mediante puertas traseras, rooykits, troyanos.
5. **Borrar las evidencias:** Se cubre cualquier indicio o pistas sobre las acciones que se realizaron en las pruebas.

Habilidades de un hacker ético

Un individuo que es un hacker ético posee un gran reto debido que debe tener amplio conocimiento de sistemas operativos, poseer comprensión en la topología de la red: hardware, software, conocimientos amplios de seguridad y de los diferentes ataques. (UNIR, 2020)

2.7 Vulnerabilidad

El mundo tecnológico en el que nos encontramos en la actualidad posee una constante innovación y evolución de manera acelerada que es imposible contar con la protección mínima para cualquier tipo de amenaza cibernéticas que pueden llegar afectar a las entidades con multas o demandas, pérdidas de activos y negocios. Es por esto de la importancia de establecer las medidas de ciberseguridad que protejan las instituciones corporativas. (Ballesteros, 2018)

2.8 Virus informáticos

Son programas generalmente destructivos, que se introducen en el ordenador (al leer un dispositivo extraíble o al ingresar a una red de Internet), que pueden provocar la pérdida de información almacenada en el disco duro o el mal funcionamiento del ordenador. Las mayores incidencias se dan el Sistema Operativo Windows debido a: Su gran popularidad entre los ordenadores personales, este gran renombre basado en la facilidad de uso sin conocimiento previo.

La falta de seguridad en esta plataforma ha hecho que Microsoft esté dando en los últimos años mayor prioridad. Lo importante es mantener protegida a la computadora (Antivirus, Firewall), una vez infectada la computadora con un virus la primera necesidad es eliminarlo sin tomar en cuenta el tipo o método de infección.

Al virus informático se los ha definido como aquellos programas informáticos que perjudican el funcionamiento del equipo. Dependiendo de su programación algunos virus pueden ser malignos y otros no tanto. (Torres, 2021)

2.8.1 ¿Qué ocurre con los virus informáticos?

Hay demasiados modos de codificación binaria de ficheros para transmitirlos a través de la red y también existen diferentes arquitecturas y virus que intentan ingresar a través de ellas. En el tema de los virus, la mayor responsabilidad recae casi siempre en los usuarios de la red, los cuales deberían tener gran control sobre los programas que ejecutan y en qué lugar se encuentran instalados.

2.8.2 ¿Cómo se producen las infecciones informáticas?

Existen dos grandes clases de producir las infecciones:

Los virus informáticos se difunden cuando las instrucciones o código ejecutable pasan de un ordenador a otro, o por medio de un dispositivo (flash memory, discos duros, cd 's).
Los virus funcionan, se reproducen y liberan sus cargas activas cuando se ejecutan, normalmente un usuario no ejecuta algún código informático, sin embargo, los virus engañan sensatamente al sistema operativo o al usuario informático para que lleve a cabo el programa viral.
El programa malicioso actúa replicándose a través de las redes como es el caso de los gusanos informáticos.

2.9 ¿Qué es el Phishing?

Se habla de phishing a una técnica muy utilizada por gente delictiva para realizar ciberataques tratando de manejar nuestros datos personales, monetarios, bancarios y las cuentas personales. Esto no ha sucedido recientemente, ya lleva muchos años entre nosotros, pero ha sido más notorio porque va tomando fuerza en sus ataques generando más víctimas.
La definición de phishing viene de la palabra inglesa fishing significa pesca, surge de la manera en que se ataca a las víctimas hasta que piquen el cebo.
También se lo ha definido como la capacidad de manipular a los usuarios para que comparta su información de manera personal por medio de chantajes recibiendo mensajes en su correo electrónico. El mensaje hace que la víctima realice un clic en el sitio web y así el hacker pueda descargar la información. (Malwarebytes, 2021)

2.9.1 Funcionamiento del phishing

Los ciberataques se inician cuando se envía un correo haciéndose pasar por una entidad u organización como bancos entre otros. En este correo se menciona que existe algún problema y que se debe solucionar amenazando un bloqueo de cuentas o tarjetas de crédito y para solucionar se debe hacer click en un link.
Al ingresar a este se descargará un malware a su ordenador donde se accederá a la información almacenada en él. Se consideran otras maneras de ataque por mensajería, redes sociales o llamadas. (AVAST, 2022)

2.9.2 Cómo protegerse del Phishing

Constantemente los sistemas operativos deben actualizarse reforzando la seguridad:

- Jamás introducir datos específicos en un link.
- Tus cuentas deben vigilarse periódicamente
- Ver el URL del enlace.

- Al ver algo extraño comunicarse con la entidad a cargo ya sea un banco.
- No descargar ningún archivo. (OCU, 2022)

2.9.3 Técnicas para combatir el phishing

Varias técnicas existen de acuerdo con la creación de tecnologías.

a) Respuestas organizativas: Capacitar a empleados para que identifiquen un ciberataque.

b) Respuestas técnicas: Implementar programas informáticos anti-phishing que evitaran que los navegadores web abran estos links.

c) Respuestas legislativas: Es una manera de usar conocimientos y llevar a juicio a los phishers sospechosos. (Ibáñez y Almenara, 2016)

2.10 Bases de datos y su manejo

Hay que considerar que muchas entidades manejan información de un gran valor por esto es necesario tenerlas en un formato ordenado y un nivel de acceso autorizado.

Las bases de datos recopilan datos, organizan y los relacionan; de esta manera hay una aceleración en su búsqueda y se pueden sacar informes de datos complejos. Existen diferentes tipos de datos:

- **Base de datos relacional:** Almacena información donde se tenga acceso a consultar, actualizar, analizar y sacar datos; utilizando tablas y campos.

  Sistema de gestión de base de datos: Software que facilita la creación y acceso a los datos con un lenguaje para acceder y manipular estos como MySQL.
- **Base de datos distribuida:** Gran disponibilidad de los datos debido a sus múltiples ubicaciones. El problema radica en la duplicación de datos y un menor nivel de seguridad.

Se clasifica en 2 tipos:

a) Homogénea: presenta un mismo esquema y sistema de gestión de base de datos. Usados en la misma institución y por esto tienen el mismo DBMS.

b) Heterogéneas: Se utilizan en diferentes empresas y organizaciones con su propio DBMS y es posible que no se sepa sus otras ubicaciones.

- **Base de datos NoSQL:** Utilizada para proyectos que trabaja con base de datos de un gran volumen su lenguaje SQL sus atributos están en una misma columna como, por ejemplo: JSON (*JavaScript Object Notation*); CQL (*Contextual Query Language*); o GQL (Graph Query Language). Presenta restricción por el alto volumen de datos que se maneja. (TicPortal, 2019)

Ransomware o secuestro de datos

Hackea y bloquea un dispositivo encriptando archivos, evitando el control del usuario en cuanto a su información y datos almacenados. Normalmente este es transmitido por un troyano. Los delincuentes piden un monto por la recuperación de documentos.

Troyano Programa de software malicioso

Este virus informático se camufla como herramienta útil. Siendo un ataque de ciberseguridad peligroso debido a que se descargan información importante del usuario.

Es necesario informarse de una manera adecuada para enfrentar un ciberataque con información valiosa se podrá proteger bases de datos de entidades para que no sean vulneradas. Nunca se debe intentar resolver en caso de que ya exista un ciberataque y jamás dejar desprotegidos archivos confidenciales es recomendable dejar la ciberseguridad en manos expertas que puedan ayudar el impacto de cualquier ataque a una organización. (Muñoz, 2021)

2.11 Antiphishing

Son aquellos programas utilizados para detectar aquel contenido que se infiltra en los sitios web como phishing. Lo importante de este software es bloquear datos y contenido para que no tenga libre acceso. (AVAST SOFTWARE, 2022)

2.12 Ciberataque

Se caracteriza por una ofensa contra sistemas de información, dañando, alterando o destruyendo organizaciones y anulando servicios. Se los clasifica en:

- Phishing attacks
- Malware attacks
- Web attacks

2.13 Procesos académicos

Se define como un procedimiento de socialización donde se interactúa la educación hacia un individuo y su desarrollo con su entorno. Varios son los procesos académicos que implican como:

Estratégicos: Se relaciona a la calidad de la educación orientando técnicas y estrategias que abarcan la evaluación académica, docente y registros de las calificaciones.

Docencia: Son aquellas actividades que implican la elaboración de programas, gestión y fortalecimiento académico para estudiantes y docentes.

Investigación: Implican proyectos relacionados a la investigación de la institución o entidades externas que las apoyen.

- Apoyo Académico: Se refiere a la gestión académica y mediaciones pedagógicas.
- Apoyo Integral: Son aquellos procesos internos de la institución y becas para estudiantes. Además de otras documentaciones para procesos académicos importantes de una institución. (Medina, 2016)

2.14 Políticas de seguridad

Las políticas de seguridad son aquellos procedimientos o serie de normas, reglas y directrices que permiten a una institución proteger su información dentro de su organización detectando, previniendo o riesgos que puedan afectarla; y dándole importancia a la ciberseguridad. Además, se ha definido como una política de seguridad a un control que va implementando una entidad. Esta surge a través de un conjunto de procedimientos o técnicas que utilizan aquella medida que se instauran para dar el complimiento de esta. Como tal una política de seguridad se basa en una caracterización y un previo análisis de los riesgos a los que llega estar la información de manera expuesta y debe incluir procesos, sistemas y personal presente en la organización. La información es mostrada a la dirección de la institución y comunicada a todo el personal. Para establecer una política de seguridad se analizará las normas ISO normas estándares otorgadas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). (Pilamunga, 2019)

2.14.1 Parámetros para crear políticas de seguridad

Cuando una organización ha decidido crear sus políticas de seguridad informática se toman en cuenta algunos aspectos:

- Realizar un análisis de los riesgos informáticos que puede llegar a presentar la institución y de esta manera mejorar políticas en la empresa.
- Se requiere informar a todos los departamentos de la organización, para poder definir el alcance y aquellas infracciones a las prácticas.
- Todos los miembros de la organización serán informados del desarrollo de las políticas, los beneficios que se otorgan y los riesgos.
- Se debe realizar monitoreos de manera habitual a procesos y operaciones de la organización y realizar cambios de manera oportuna.
- Especificar el alcance que tendrán las políticas al instaurar los mecanismos de seguridad que respondan a las políticas trazadas. (Departamento de Tecnología Organización Inca, 2018)

2.14.2 Buenas prácticas

El documento de buenas prácticas de seguridad de la información se refiere aquellas cláusulas que se encuentra agregado en el contrato de los trabajadores y aquellas directrices donde los equipos de trabajo mantengan protegida su información con el bloqueo de su equipo si se encuentra desatendido.

Los procedimientos de control de accesos proporcionan medida de técnicas y organizativas que otorga un permiso al sistema donde se encuentra almacenada la información de la institución y su acceso. La manera de controlar el ingreso puede ser, por ejemplo:

- Controles de acceso físico: Se dice de aquel mecanismo que permite limitar el acceso aquellas personas a la organización a través de barreras, cámaras, alarmas o un sistema biométrico, de esta manera se impide el acceso no autorizado.
- Controles de acceso lógico: Aquel sistema que permite guardar información y vigilar el ingreso de los usuarios como la configuración de permisos de lectura y escritura o aquellos sistemas de login.
- Procedimientos de gestión de usuarios: Se debe proceder, accesos y permisos para aquellos trabajadores que puedan manejar la información de la organización y que su desempeño sea óptimo en el trabajo, así se debe manejar la concesión de los permisos de acceso tanto físico como lógicos en la entidad.
- Procedimiento de clasificación y tratamiento de la información: Se debe clasificar la información considerando valor, requisitos legales, sensibilidad y criticidad de la institución y las medidas a tomar para poder proteger y manipular la misma.
- Procedimiento de gestión de incidentes de seguridad de la información: Tomar en consideración las notificaciones de aquellos incidentes y la acción a tomar.
- Otros procedimientos: La implementación de copias de seguridad de la base de datos, seguridad presente en la red, antimalware, entre otros. (UNIR, 2020)

2.15 Normas ISO 27000

Un Sistema de gestión de la seguridad de la información agrupado aquellas políticas y procedimientos que sirven para estandarizar la gestión de la Seguridad de la Información en una organización. Varias entidades han decidido ser parte y colaborar con el desarrollo de las normas. A continuación, se muestran algunos detalles de los estándares que están incluidos en esta norma ISO:

- ✓ ISO 27000: Conjunto de políticas que abarca términos de todas las normas de la familia.
- ✓ ISO 27001: abarca aquellos requisitos para un SGSI. Incluye en la lista el ciclo de mejora continua.

- ✓ ISO 27002: Reúne buenas prácticas para la Seguridad de la Información. Cuenta con 14 dominios,35 objetivos de control y 114 controles.
- ✓ ISO 27003: Una guía de un SGSI. Convirtiéndose en apoyo de la norma 27001. Esta normativa toma el modelo de procesos de planear-hacer-chequear-actuar (PDCA).

Tabla 1-2: Modelo PDCA aplicado a los procesos de SGSI

Planificar (Establecer el SGSI)	Se determinan políticas, procesos y procedimientos, con el fin de ver las políticas que se encuentran establecidas por la organización.
Hacer (Implementar y operar el SGSI)	El fundamento es implementar controles y su adecuado uso.
Verificar (Revisar y dar seguimiento al SGSI)	Se establece y verifica el desempeño de aquellos procesos, objetivos en cuanto a seguridad y reporte de resultados a la dirección.
Actuar (Mantener y mejorar el SGSI)	La toma de acciones para corregir y prevenir de acuerdo con la verificación en cuanto a la dirección, para la mejora continua del SGSI.

Fuente: (Valente, 2018)

Realizado por: Marco Estrada. 2022

2.16 ISO 27000

Muchos países han decidido formar parte y participar en conjunto con la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional que han creado estándares para obtener un buen sistema de gestión de seguridad de la información; es decir que ésta norma orienta y da facilidad continua y evita riesgos. De esta manera está norma es funcional para todo tipo de empresas públicas o privadas.

2.17 ISO 27001

La Organización Internacional de Estandarización fijó la norma ISO 27001 para certificar aquellos sistemas de gestión de seguridad de la información de aquellas entidades empresariales. La normativa detalla requisitos para poder evitar que se pierda información. Esta norma fue establecida en el 2013 y revisada y publicada en el 2005.

Toda organización tiene derecho de utilizar la norma ISO 27001 y la misma concede un plan de seguridad para ser aplicada la gestión de seguridad de la información.

El principal objetivo es otorgar que la información sea segura y mejorarla, reduciendo los riesgos que interfieran en el sistema de información de las empresas y la apertura de mantener protegida a la información.

Surgen ventajas esenciales para implementar esta norma:

- Cumplir con los requerimientos legales: Efectuar con las normativas similares con la seguridad de la información debido a que las normas establecen una metodología.
- Obtener una ventaja comercial: la perspectiva se ve favorecida al compararlas con otras universidades.
- Menores costos: se evita incidentes de seguridad.
- Una mejor organización: implementada la norma ISO 27001 se logra mejorar procesos y procedimientos disminuyendo el tiempo que no han logrado cumplir sus empleados. (CTMA consultores, 2021).

2.17.1 Estructura de la norma ISO 27001

Esta normativa está estructurada de la siguiente manera:

1) **Introducción:** Al encontrarse de manera abierta la información está expuesta, por lo que se ve necesaria tratar para no tener fugas de información.
2) **Alcance:** el SGSI determina con sus requisitos que es usado para cualquier tipo de institución.
3) **Normativas de Referencia:** Específica como referencia de carácter obligatorio a la normativa ISO/IEC 27000.
4) **Términos y definiciones:** Se establece una guía en cuanto a los términos con sus definiciones.
5) **Contexto de la Organización:** La entidad se ve en la obligación de establecer, implementar, mantener y realizar mejoras constantemente.
6) **Liderazgo:** Se establecen responsabilidades y funciones de la alta dirección siguiendo el régimen de SGSI.
7) **Planificación:** Se realizan una identificación, análisis y planificación en cuanto a los riesgos de la información.
8) **Soporte:** Con la información almacenada es posible controlar y conservar documentos del SGSI.
9) **Operación:** Evaluar los riesgos que puede tener la seguridad de la información utilizando un programa.
10) **Evaluación del rendimiento:** Es necesario realizar una auditoría para controlar que la información está de forma segura.
11) **Mejora:** Utilizando una auditoría se verifican resultados.

2.18 SGSI

Los Sistemas de Gestión de la Información o SGSI, se refiere aquella técnica que facilita a las organizaciones o entidades que muestra los activos de la empresa está siendo manejada de forma correcta y no existe ningún riesgo de que la información se esté fugando. Se basa en evaluar aquellos riesgos y la manera en que la organización trata y la mejora de manera asertiva.

Principios fundamentales para que el SGSI sea implementado con éxito a la empresa:

- ✓ Tener conocimiento de la implementación de la seguridad de la información.
- ✓ Asignación de responsabilidades.
- ✓ El compromiso de la dirección y de todas las partes.
- ✓ El nivel aceptable de riesgo una vez que ha sido evaluado
- ✓ Prevención activa y la visualización incidente de seguridad de la información
- ✓ Verificar de manera constante la seguridad de la información y lo que se ha ido modificando.

Las empresas siempre se encuentran vulnerables ante cualquier potencial riesgo, y expuestas a cualquier amenaza. Para lo cual es necesario verificar el nivel de riesgo al que se encuentra expuesta la información de la organización y se debe eliminarla llegando a un nivel cero de que se produzca.

Aunque se ha analizado que el riesgo no se ha podido eliminar en la totalidad, las entidades pueden monitorear y tratar de controlarlo reduciendo el riesgo. (Pilamunga, 2019)

2.19 OWASP

Se menciona aquella organización que no lucra y está conformada por miembros voluntarios; además que el trabajo que realizan es entregado por los patrocinadores.

Los recursos gratuitos son publicaciones, artículos, normas, software de testeo y capacitación, capítulos locales y listas de correos; otorgada por patrocinios. De acuerdo con sus siglas en inglés significa Open Web Application Security Project promueve y orienta servicios web. Se destaca que cualquier persona natural puede participar en OWASP en todas las actividades mencionadas anteriormente.

Las publicaciones con mayor aceptación han sido: top 10 vulnerabilidades de aplicaciones Web, guía de desarrollo seguro de aplicaciones Web, proyecto legal, proyecto de métricas y medidas, App Sec FAQ; pueden ser buscadas con facilidad en la web de la página oficial de OWASP. (Fernández, 2010)

2.20 OWASP Top 10

La definición de acuerdo con sus siglas son Open Web Application Security Project un documento que muestra las vulnerabilidades críticas en la web. Su objetivo prioritario ha sido enseñar a profesionales de las organizaciones sobre aquellas debilidades de las páginas web. En el transcurso de los años OWASP Top 10 ha requerido actualizarse y se lo ha rediseñado como, por ejemplo: *JaveScript* un lenguaje de secuencias principal de la web y los frameworks web estableciéndose en el cliente. Así los riesgos en aplicaciones web se clasifican según OWASP top 10.

El principal riesgo del OWASP Top 10 ha sido mostrar el riesgo crítico para la gran gama de instituciones, proporcionando información genérica sobre la probabilidad y el impacto técnico; a través de un esquema calcular el impacto del riesgo.

Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

Figura 2-2: Esquema de evaluación de riesgo de OWASP.

Fuente: OWASP Top 10,2017

Aquellos nombres de riesgo se encuentran establecidos en el marco de debilidades del CWE y así mejorar la seguridad aceptada y disminuir alguna confusión.

2.20.1 Riesgos en Seguridad de Aplicaciones OWASP Top 10 2017

a) **A1: 2017 Inyección**

Vulnerabilidad que de manera directa va a las bases de datos. El atacante logra manipular al usuario para que se altere el funcionamiento y lograr extraer información. Para evitar este tipo de inyección es necesario usar una API segura y usar una interfaz parametrizada.

b) **A2: 2017 Pérdida de Autenticación**

Muchas cuentas administrativas se ven afectadas por atacantes al tener acceso a los usuarios y contraseñas debido a la fuga de información. Así los atracadores necesitan el acceso de pocas cuentas y afectar el sistema. Para evitar este tipo de ataques es necesario implementar el control de contraseñas débiles, se puede incrementar el tiempo de respuesta a cada fallo al iniciar sesión. (Pinango, 2021)

c) **A3: 201 Exposición de datos sensibles**

Se ejecutan ataques Man in the Middle o se roban datos en texto plano del servidor. Este tipo de ataques presenta mayor impacto por la presencia de datos sensibles. Para evitar

estos sucesos es necesario clasificar datos procesados, almacenados en el sistema y mantener un control para cada clasificación.

d) A4: 2017 Entidades Externas XML (XXE)

El atacante identifica un vector ataque como explotar procesadores XML antiguos. Mediante herramientas SAST se visualizan estos inconvenientes. Los defectos se usan para extraer datos. Las aplicaciones son débiles y sobre todo aquellos servicios web basados en XML de fuentes no seguras. Una manera de prevenir este tipo de vulneración es utilizar formatos como JSON e impedir que el código de datos propio de las entidades.

e) A5: 2017 Pérdida de Control de Acceso

La explotabilidad para poder controlar los accesos de atacantes que puede ser detectable de manera manual. Aquellas debilidades de control de acceso no se detectan por pruebas automatizadas, estáticas como dinámicas. Para prevenir el control de acceso se reconoce la eficiencia si es aplicada del lado del servidor donde el acceso no se ve modificado por el atacante. (OWASP, 2017)

f) A6: 2017 Configuración de Seguridad Incorrecta

La manera de permitir configuraciones establecidas o aquellos encabezados HTTP mal configurados que presentan datos dedicados. Los mismos que son configurados de manera segura y actualizarse de manera constante.

g) A7: 2017 Secuencia de Comandos en Sitios Cruzados (XSS)

Ocurren debido a que los XSS seleccionan datos no confiables y los emiten hacia el navegador web sin validación y codificación apropiada. Existen tres formas de ataque:

XSS Reflejado: Utiliza datos donde la víctima debe dar click en un enlace o página administrada por el atacante como publicidad.

XSS Almacenado: Acumula la información del usuario, el problema es que queda visible para otros usuarios, considerado como un problema de alto riesgo.

XSS Basados en DOM: Basado en APIs no seguras que son controladas por el atacante.

Para evitar que surjan estos inconvenientes lo mejor es separar la información no confiable del contenido del navegador.

h) A8: 2017 Deserialización insegura

Las APIs llegan a verse vulneradas cuando surge un ataque a la estructura de datos y objetos modificando el comportamiento de la aplicación y deserializandola. Una manera de evitar esto es restringir y monitorear conexiones de red que sepan utilizar funcionalidades de deserialización.

i) **A9: 2017 Componentes con vulnerabilidades conocidas**

Surge cuando existe una falta de funcionalidad en el sistema y es difícil detectar algún ataque, ocasionando la pérdida de datos o la adquisición del servidor. Se ven vulneradas aquellas aplicaciones que debilitan sus defensas teniendo impactos significativos.

j) **A10:2017 Registro y Monitoreo Insuficientes**

Al no tener una rápida respuesta en cuanto surge un ataque en el tiempo, los delincuentes pueden extraer la información o manipularla a su antojo. Se ha considerado que existe una detección de seguridad mayor a 200 días. (OWASP, 2017)

2.21 NMAP (Network Security Scanner)

Se menciona aquella herramienta opensource comúnmente usada para el escaneo de red, puertos y vulnerabilidades que son útiles para la entrada de sistemas. Fue creada para realizar un escaneo de grandes redes, a pesar de que logra escanear un simple host.

Aquellas técnicas de escaneo que usa Nmap han sido conjugadas ya para sistemas de detección de intrusos y firewalls.

Algunas de las funciones que se pueden aplicar con NMAP son:

- Reconocer aquellos dispositivos vinculados a la red.
- Notar puertos abiertos, sistemas operativos en ejecución a través de estándares de uso de puertos.
- Encontrar programas en peligro presentes en la red.

Determinando hosts disponibles en la red

Se determinará si un host está activo antes de que el mismo sea escaneado.

Para realizar esto se consideran varias técnicas como son:

- TCP conncet()-sT
- UDP-sU
- ICMP Echo(Ping sweep) Scan-sp
- Avanzados
    - ★ Fin-sF
    - ★ Null-sN
    - ★ Xmas-sX (Gómez, 2019)

Tabla 2-2: Opciones Adicionales del NMAP

Opción	Acción
-oN	Enviar la bitácora a un archivo
-iL	Tomar targets desde archivo
-p	Especificar rango de puertos
-g	Especifica el número de puerto de origen
-F	Solo escanear puertos especificados
-S	Spoofing de dirección IP,enmascara de dirección IP fuente, a cargo de Ethernet.

Fuente: (Gómes, 2018)

Realizado por: Marco Estrada. 2022

2.22 NIKTO

"Nikto, también es llamado como Nikto2, su servidor web de código abierto y gratuito realiza un escaneo de vulnerabilidades buscando archivos, errores de configuraciones en los servidores, versiones de software desactualizados, programas con código malicioso, y varios elementos que puedan ser un tipo de peligro para todos los servicios web de alguna página en específico. Entre las principales características tenemos:

- Actualizaciones frecuentemente, uso gratuito y de código libre.
- Puede escanear cualquier servidor con programación web apache, litespeed, niginx, etc.
- Indica si existen directorios abiertos dando una breve descripción, se ven los encabezados de la programación indicando informes inusuales.
- Posee la capacidad de escanear certificados SSL
- Los puertos son revisados por un proxy con autenticación (CIBERSEGURIDAD, 2020)

2.23 HPING3

Linux dueño de esta aplicación que permite analizar las trayectorias y reconstruir los pagues de la tecnología TCP/IP. Envían paquetes tipo TCP, RAW-IP, UDP analizando y utilizando para fines de seguridad.

Es muy utilizada en firewalls porque detecta paquetes sospechosos ideal para la protección de ataques DOS.

Sirve el HPING3 para probar redes y host, pero las principales utilidades son:

- Pruebas de red comprobando la utilidad de diferentes protocolos.

- Con los protocolos admitidos se realiza un traceroute avanzada de forma rápida.
- Importante para realizar escaneo de puertos.
- El sistema operativo con una huella digital remota.
- Comprobar el funcionamiento del firewall
- Auditorías de protocolos de red. (Gómes, 2018)

CAPÍTULO III

3 DISEÑO DE LA INVESTIGACIÓN

3.1 Tipo y diseño de la investigación

Este proyecto es de carácter investigativo y experimental, mediante la bibliografía recabada; sirve de fundamento de los diferentes métodos y técnicas, para realizar un análisis de resultados.

3.1.1 Tipo de Investigación

El presente estudio es de tipo explicativo cuyo fin es encontrar el problema y comprenderlo de manera eficiente para implementar y evaluar un sistema de seguridad anti-phishing para proteger la información utilizando un Firewall para los procesos académicos en línea para el Instituto Superior Tecnológico Riobamba.

3.1.2 Diseño de la investigación

Para el diseño de esta investigación se ha decidido utilizar un estadístico aplicando la prueba de Chi-Cuadrado (x^2). Donde se consideró evaluar la plataforma académica del Instituto Superior Tecnológico Riobamba, analizando 7 de las vulnerabilidades de las existentes detectadas por la nueva plataforma, mismas que se detectó a través del software OWASP.

3.2 Métodos y técnicas de investigación

3.2.1 Método científico

Los pasos para la presente investigación son los siguientes:

1. Obtener una fuente bibliográfica para tener considerable material teórico (Registros, Internet, bibliografía científica, investigaciones realizadas en el país y estadísticas oficiales).
2. Formulación de la hipótesis
3. Experimentación: Se realizará distintos casos para comprobar que la implementación de un firewall es una gran solución para controlar el tráfico que soporta el sistema académico del Instituto Superior Tecnológico Riobamba.
4. Análisis de la información, exacta y real, creando posibles soluciones para la toma de decisiones y generando recomendaciones a las diferentes áreas que manejan el sistema académico del Instituto Superior Tecnológico Riobamba.

5. Comprobar la hipótesis: con la instalación del firewall en la red del Instituto Superior Tecnológico Riobamba, aumenta el nivel de seguridad en toda la plataforma académica institucional.

3.3 Instrumentos de recolección de datos

Las herramientas utilizadas para la experimentación y recolección de datos serán las siguientes:

3.3.1 NMAP

Esta herramienta se utilizará para realizar acciones como:

- Identificación de servicios
- Detección de direcciones IP
- Detección de sistema operativo
- Escaneo de puertos

3.3.2 OWASP

Owasp Zap como herramienta para pruebas de penetración y detección de vulnerabilidades en aplicaciones o servicios web, permitirá realizar una auditoría de seguridad de nuestro servidor Web, el cual nos emitirá un informe total acerca de las vulnerabilidades encontradas. Se escaneará todo el servidor web haciendo peticiones GET y POST para detectar posibles vulnerabilidades en la aplicación.

3.3.3. HPING3

Utilizaremos esta herramienta para realizar un ataque de Denegación de servicio DoS mediante un hping3 en el modo Flood.

3.3.4. NIKTO

Utilizaremos esta herramienta para examinar el sitio web www.itsriobamba.com para que se realice un informe de vulnerabilidades logrando utilizar para explotar o hackear el sitio.

3.3.5 Navegadores de Internet

Para poder ingresar a los sitios web que realizaremos las pruebas en la investigación utilizaremos varios navegadores como Google Chrome, Mozilla Firefox, Microsoft Edge.

3.3.6 Kali Linux

Se ha decidido recolectar información mediante el uso de Kali Linux debido que es muy usado por su seguridad informática aplicando herramientas con las que se puede obtener una seguridad del sistema.

3.4 Fuentes de información

Las fuentes que serán utilizadas en el presente estudio de investigación son las siguientes:

- **Primaria:**

La principal fuente obtenida por el investigador es la que ayuda a comprobar la hipótesis, y los problemas que se constatan en el sistema académico.

- **Secundaria:**

1) Artículos en revistas científicas, relacionados al tema de investigación.
2) Sitios especializados en ciberseguridad y páginas oficiales en software aplicados al diseño de seguridad web.
4) Material online encontrado en bibliotecas electrónicas referentes al tema.

3.5 Planteamiento de la hipótesis

3.5.1 Hipótesis general

La implementación de un sistema de seguridad anti-phishing con firewall mediante software libre mejorará la integridad y confidencialidad de la información en los sistemas en línea del Instituto Superior Tecnológico Riobamba.

3.5.2 Identificación de variables

- **Variable independiente:** Sistema de Seguridad anti-phishing.
- **Variable dependiente:** Amenazas y fallas del sistema de seguridad en la plataforma institucional.

3.5.3 Operacionalización metodológica de variables

Tabla 2-3: Operacionalización metodológica de variables

Hipótesis	Variables	Indicadores	Técnica	Instrumento
La implementación de un sistema de seguridad anti-phishing con firewall mediante software libre mejorará la integridad y confidencialidad de la información en los sistemas en línea.	**Independiente** Sistema de Seguridad anti-phishing utilizando un Firewall. **Dependiente** Amenazas y fallas del sistema de seguridad en la plataforma institucional.	Equipamiento Software / Aplicaciones Datos N° de vulnerabilidades encontradas en la plataforma	Observación Observación	Pruebas Programas de escaneo de amenazas y vulnerabilidades del sistema.

Fuente: (Espinoza, 2019)

Realizado por: Marco Estrada. 2022

3.6 Población y muestra

3.6.1 Población

En este estudio se consideró como población de esta investigación a la plataforma informática del Instituto Superior Tecnológico Riobamba. Utilizando la herramienta OWASP TOP 10 verificando la exposición que tiene la plataforma académica ante 7 de 10 riesgos críticos que vulneran la seguridad de la red, así como la arquitectura de la programación de la plataforma institucional.

3.6.2 Selección de la muestra

Para seleccionar una porción representativa de la población, que permita generalizar los resultados de la investigación y por motivos de factibilidad relacionados con la disponibilidad de recursos se establece una muestra del tipo probabilístico, para esta investigación la plataforma del Instituto Superior Tecnológico Riobamba, determinando como muestra 7 de 10 vulnerabilidades en el OWASP Top 10, obteniendo que 7 vulnerabilidades tienen relación con el presente estudio de investigación.

3.7 Metodología para evitar vulnerabilidades en plataformas informáticas

Para realizar la metodología y estudio se ha basado en el "test de penetración de explotación de vulnerabilidades con Metasploit-framework" que menciona 3 etapas de pruebas:

Fase 1: Recopilar información

Fase 2: Análisis y explotación vulnerabilidades

Fase 3: Generar informes (Pinango, 2021)

3.7.1 Fase 1: Recopilar información

Para llevar a cabo la compilación de información por parte de la institución y realizar el estudio necesario en la plataforma académica informática del Instituto Superior Tecnológico Riobamba siendo que ésta es vulnerable en su seguridad web, por lo que se empleó técnicas para verificar las amenazas y vulnerabilidades de la infraestructura del sitio, tomando en cuenta el área de TICS principalmente.

3.7.1.1 *Escenario de trabajo*

La figura 1-3, muestra el escenario del presente estudio, detalla datos necesarios para seguir con la próxima etapa; sistema operativo, direcciones IP, enlaces web.

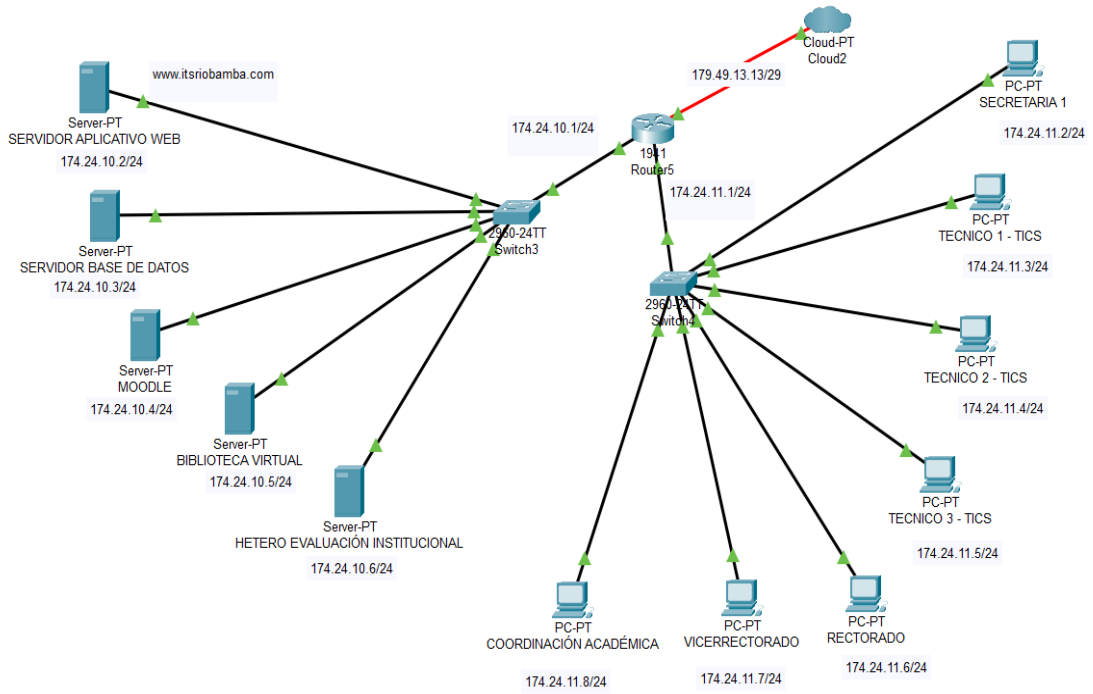


Figura 1-3. Escenario de trabajo
Realizado por: Marco Estrada. 2022

3.7.2 Fase 2. Análisis y explotación de vulnerabilidades

Al tomar como referencia la guía de los riesgos del OWASP TOP-10, se analizó que la plataforma del Instituto Superior Tecnológico Riobamba se ve afectado por las siguientes vulnerabilidades:

Tabla 3-3: Vulnerabilidades Detectadas con OWASP TOP 10

Vulnerabilidad Detectadas con OWASP
Application Error Disclosure
Exploración de Directorios
Missing Anti-clickjacking header
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion
X-Content-Type-Options Header missing
Divulgación de información-Comentarios Sospechosos

Fuente: OWASP TOP-10, 2021
Realizado por: Marco Estrada. 2022

3.7.2.1 *Herramientas para el escaneo de vulnerabilidades*

En una máquina virtual se instaló el sistema operativo Kali Linux utilizando las siguientes herramientas para detección, escaneo y problemas de programación: NMAP, OWASP, HPING3, NIKTO.

3.7.2.2 *Escaneo de vulnerabilidades*

Con las herramientas planteadas se procederá a realizar las pruebas de Testing del servidor Web del Instituto Superior Tecnológico Riobamba, con los 3 escenarios que se muestran a continuación:

Se iniciará las pruebas de penetración al servidor Web con el Escenario 1, como se muestra en la Fig. 2-3. En donde el atacante se encuentra dentro de la red LAN, donde se encuentra el servidor web. Tomando en cuenta que una vez que nos encontremos dentro de ella, usaremos todos los recursos de red para realizar el ataque, como por ejemplo el ancho de banda.

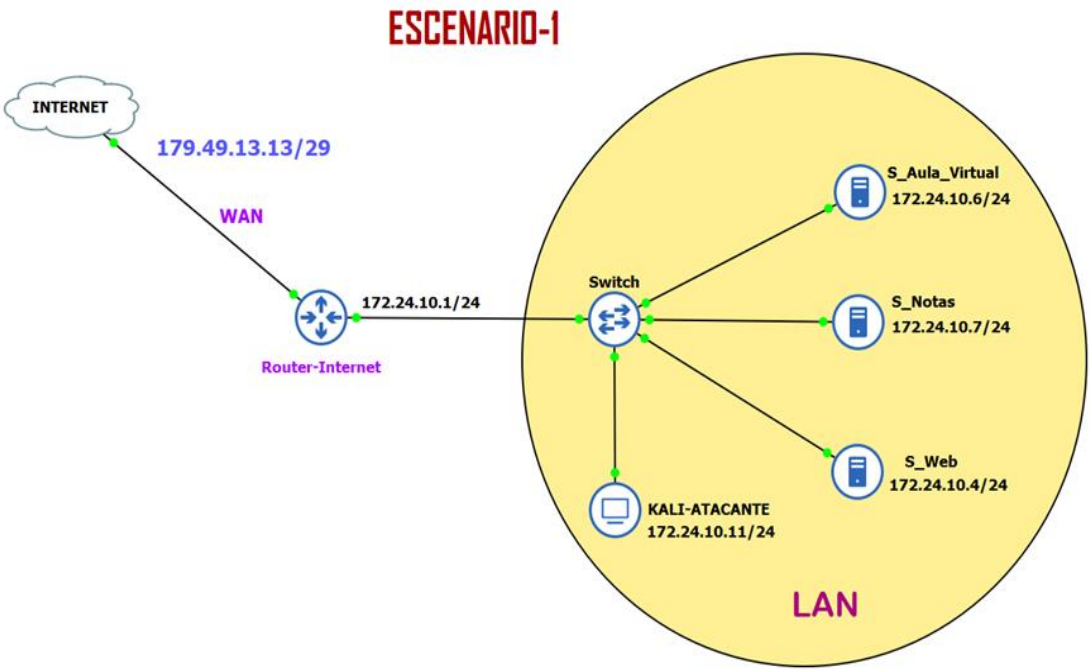


Figura 2-3. Escenario 1, para las pruebas de Testing del servidor Web
Realizado por: Estrada Marco,2022

A continuación, en la Figura 3-3 se da a conocer la dirección IP del SERVIDOR: 172.24.10.4/24

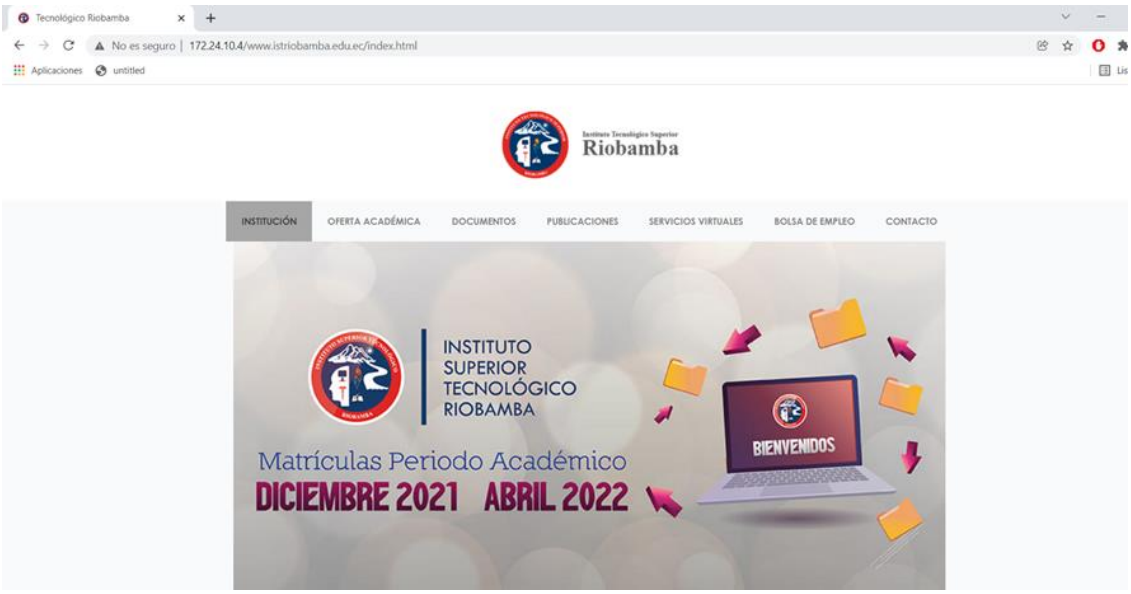


Figura 3-3: Página Web clonada.
Realizado por: Estrada Marco,2022

En la Figura 4-3 se da a conocer la dirección IP del ordenador del atacante, 172.24.10.11

Figura 4-3: Dirección IP del Atacante.
Realizado por: Estrada Marco,2022

En la Figura 5-3 se muestra la comprobación de conectividad entre el atacante y el servidor:

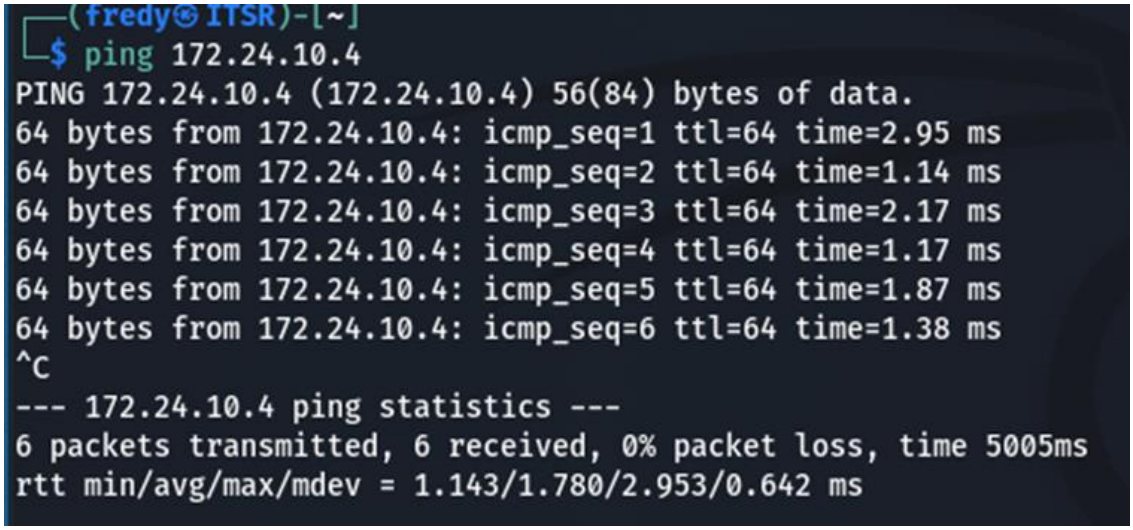


Figura 5-3: Comprobación mediante ping, entre el atacante y el servidor Web.
Realizado por: Estrada Marco,2022

- **Testing con la herramienta NMAP**

Mediante Nmap, nuestro principal objetivo ha sido poder escanear los puertos, y conocer el sistema operativo sobre el cual se encuentra el servidor web. Una vez conocido el puerto, para poder realizar un ataque DoS.

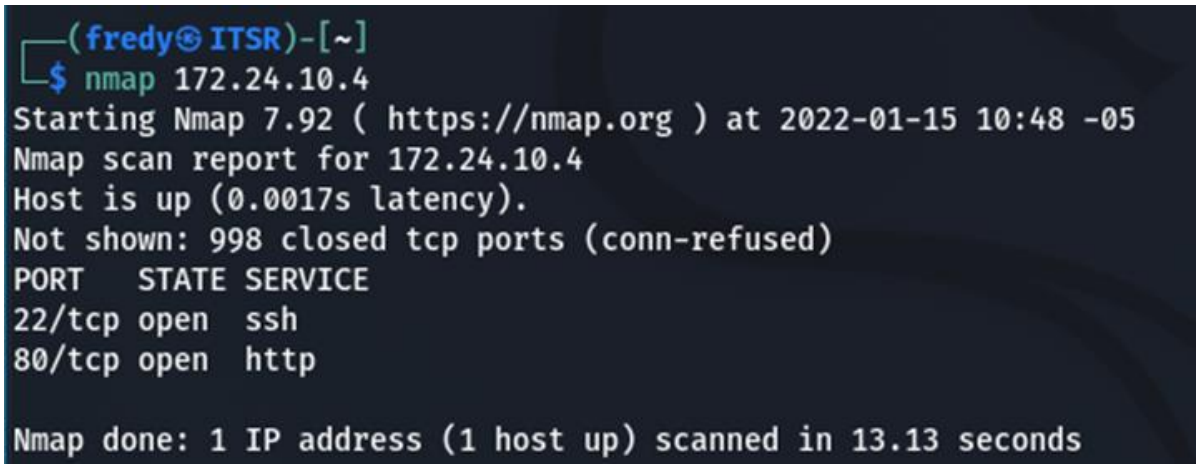


Figura 6-3: Figura Nmap-Puertos abiertos.
Realizado por: Estrada Marco,2022

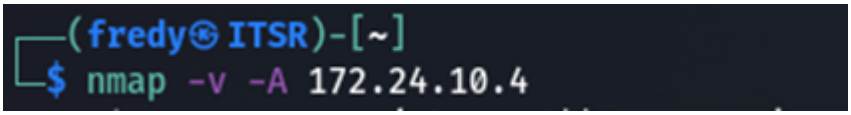


Figura 7-3: Comando para el escaneo mediante Nmap.
Realizado por: Estrada Marco,2022

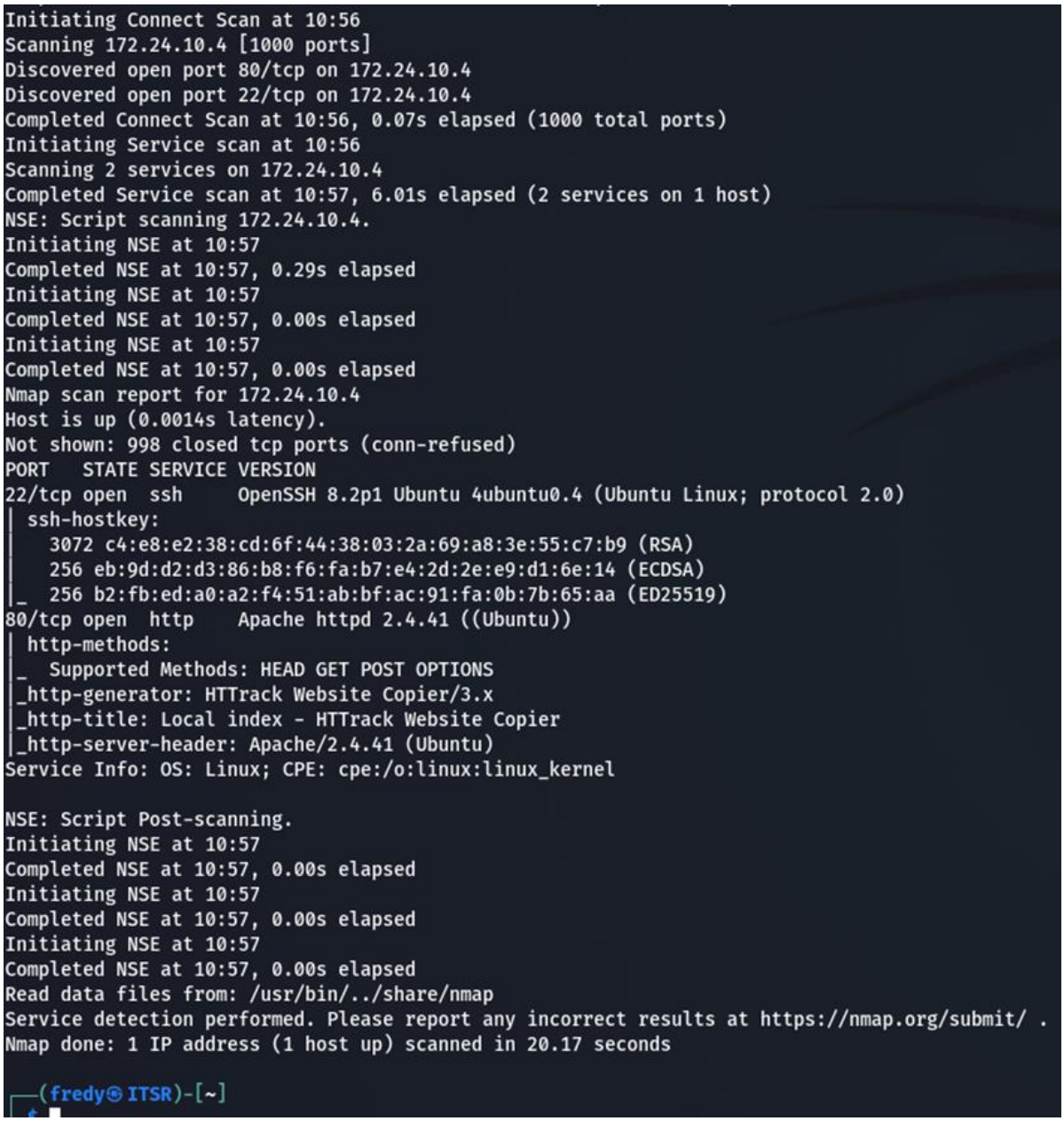


Figura 8-3: Resultados de escaneo usando Nmap.
Realizado por: Estrada Marco,2022

En la Figura 6-3 se puede apreciar que luego de realizar el escaneo usando Nmap, en primera instancia se conoce los puertos que se encuentran abiertos, en cuanto a la Figura 7-3 se visualiza el comando introducido para proceder al escaneo del servidor Web, y finalmente en la Figura 8-3 se identifica que una vez realizado el escaneo, se puede apreciar los siguientes puntos:

- Los puertos habilitados son el 22/tcp de ssh y el puerto 80/tcp de http.
- Cuenta con un OS: Linux.
- El servidor Web se encuentra montada en la distribución Ubuntu de Linux mediante Apache/ versión: 2.4.41.

- El servidor Web tiene activo el servicio de SSH a través de OpenSSH versión: 8.2p1 y adicionalmente se pueden observar las llaves de encriptación que usa el servicio.
- También se puede apreciar que el servidor Web se encuentra clonada, mediante el generador Website HTTrack.

❖ **Testing con la herramienta OWASP**

Mediante Owasp se ha procedido a realizar al nivel LAN, un análisis de vulnerabilidades o alertas que puede presentar mi servidor web, la cual una vez realizado el análisis se adjunta el informe total, con las posibles soluciones para mitigarlos. A continuación, en la Figura 9-3 podemos apreciar el proceso de ataque y revisión de vulnerabilidades.

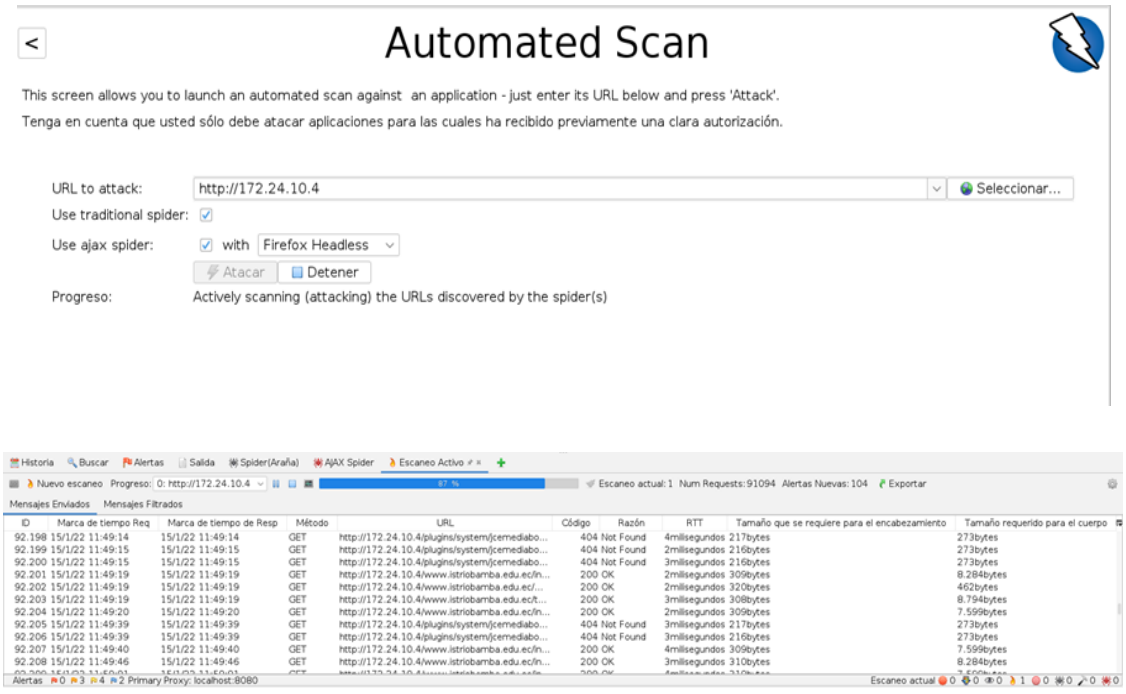


Figura 9-3: Análisis de vulnerabilidad mediante Owasp
Realizado por: Estrada Marco,2022

En la Figura 9-3, Figura 10-3 y Figura 11-3 se puede apreciar los reportes obtenidos una vez aplicado el análisis de vulnerabilidad con Owasp. En donde definen cada vulnerabilidad como alerta, la cual se encuentra categorizada por: Alto, Medio, Bajo e Informativo. En la Fig. 12-3 se puede observar los tipos de alertas encontradas, y con su respectiva estadística.

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- http://172.24.10.4

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: Alto, Medio, Bajo, Informativo

Excluded: None

Confidence levels

Included: User Confirmed, Alto, Medio, Bajo

Excluded: User Confirmed, Alto, Medio, Bajo, Falso positivo

Figura 10-3: Informativo acerca del reporte con Owasp, Escenario-1
Realizado por: Estrada Marco,2022

		Confidence				
		User Confirmed	Alto	Medio	Bajo	Total
Risk	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	0 (0,0 %)	0 (0,0 %)	741 (21,3 %)	0 (0,0 %)	741 (21,3 %)
	Bajo	0 (0,0 %)	0 (0,0 %)	2230 (64,1 %)	7 (0,2 %)	2237 (64,3 %)
	Informativo	0 (0,0 %)	0 (0,0 %)	480 (13,8 %)	22 (0,6 %)	502 (14,4 %)
	Total	0 (0,0 %)	0 (0,0 %)	3451 (99,2 %)	29 (0,8 %)	3480 (100%)

Figura 11-3: Estadística de alertas encontradas.
Realizado por: Estrada Marco,2022

Alert type	Risk	Count
Application Error Disclosure	Medio	100 (2,9 %)
Exploración de directorios	Medio	104 (3,0 %)
Missing Anti-clickjacking Header	Medio	535 (15,4 %)
Vulnerable JS Library	Medio	2 (0,1 %)
Ausencia de fichas (tokens) Anti-CSRF	Bajo	97 (2,8 %)
Cross-Domain JavaScript Source File Inclusion	Bajo	1460 (42,0 %)
Divulgación de la marca de hora - Unix	Bajo	7 (0,2 %)
X-Content-Type-Options Header Missing	Bajo	673 (19,3 %)
Content-Type Header Missing	Informativo	48 (1,4 %)
Divulgación de información - Comentarios sospechosos	Informativo	454 (13,0 %)
Total		3480

Figura 12-3: Tipos de alertas halladas, una vez testeada en el escenario 1.
Realizado por: Estrada Marco,2022

- **Testing con la herramienta HPING 3**

Localmente mediante la herramienta Hping3 se realizó el ataque DoS, tal y como se muestra a continuación, mediante la Figura 13-3.

```
┌──(fredy㉿ITSR)-[~]
└─$ sudo hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 172.24.10.4
HPING 172.24.10.4 (eth0 172.24.10.4): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Figura 13-3: Uso de la herramienta Hping3 para el ataque DoS.
Realizado por: Estrada Marco,2022

Donde efectivamente el ataque fue exitoso como se observa en la Figura 14-3, utilizando el recurso flood y así como también especificando el puerto 80 por el cual se realiza la inundación de peticiones. El tiempo empleado para que el ataque sea exitoso, fue de 4 minutos aproximadamente.

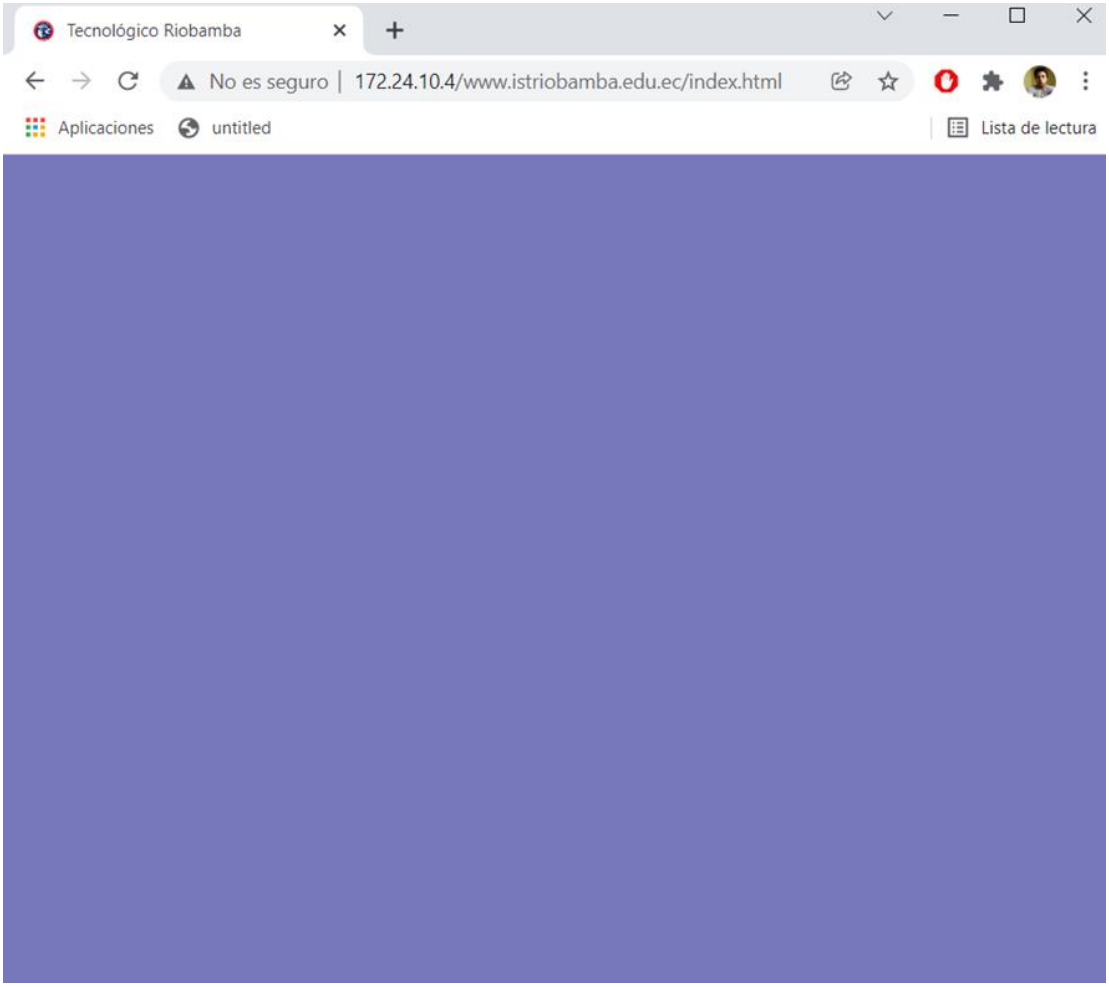


Figura 14-3: Verificación de la caída del servidor Web, una vez atacada mediante Hping3.
Realizado por: Estrada Marco,2022

Una vez verificado el ataque DoS, se procedió a cancelar la ejecución del hping3 como se aprecia en la Figura 15-3 y consiguiente aquello se procedió a verificar que la página web, se encuentre en funcionamiento.

Figura 15-3: Cancelación del ataque Hping3
Realizado por: Estrada Marco,2022

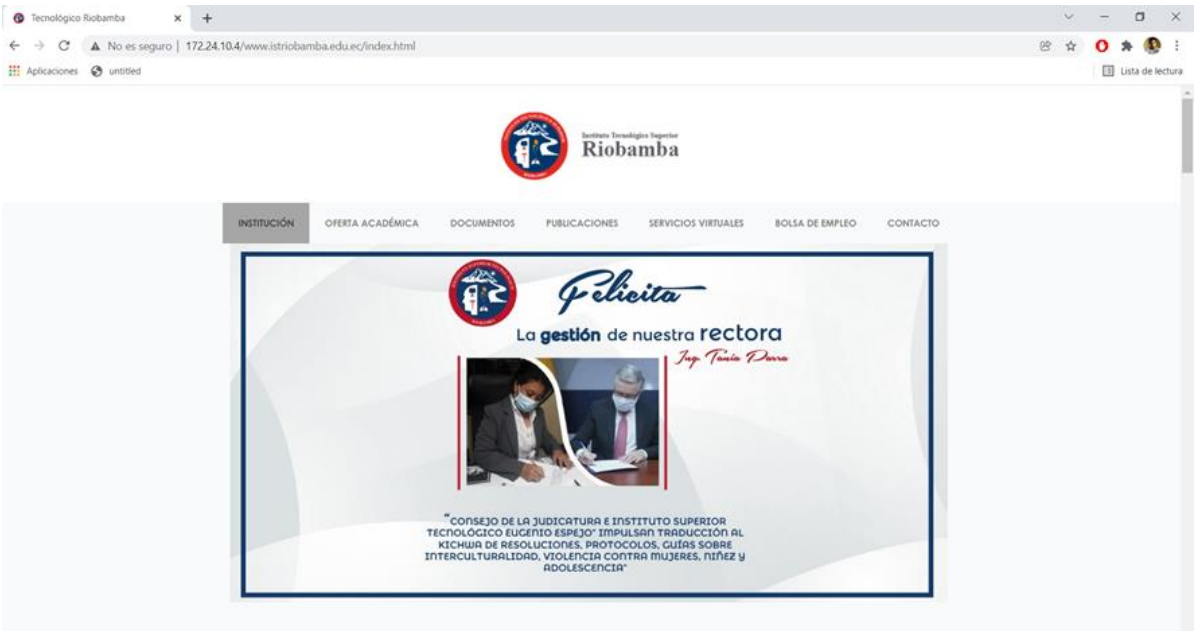


Figura 16-3: Restablecimiento del servidor Web, una vez cancelado el ataque por Hpin3.
Realizado por: Estrada Marco,2022

❖ Testing con la herramienta NIKTO

Figura 17-3: Ataque al servidor Web mediante la herramienta NIKTO
Realizado por: Estrada Marco,2022

Mediante nikto se puede evidenciar por la Figura 17-3, que además de brindar información del sistema operativo en el que se encuentra montada mi servidor web, las vulnerabilidades principales que se tiene, así como también mencionan la soluciones que se debe tomar para poder mitigarlos. En donde se pudo apreciar las siguientes vulnerabilidades:

- X-Frame-Options anti-clickjacking no está presente
- X-XSS-Protection no está definido.
- X-Content-Type-Options no está configurado. Esto podría permitir que el agente de usuario represente el contenido del sitio de una manera diferente al tipo MIME.
- OSVDB-576 (CVE-2015-1476), permite mostrar la lista de directorios con sus contenidos, actualice a v6.0 SP1 o superior.
- OSVDB-119 (CVE-1999-0269), el servidor remoto puede permitir listados de directorios a través de Web Publisher obligando al servidor a mostrar todos los archivos a través de 'exploración de directorio abierto'. Web Publisher debe estar deshabilitado.

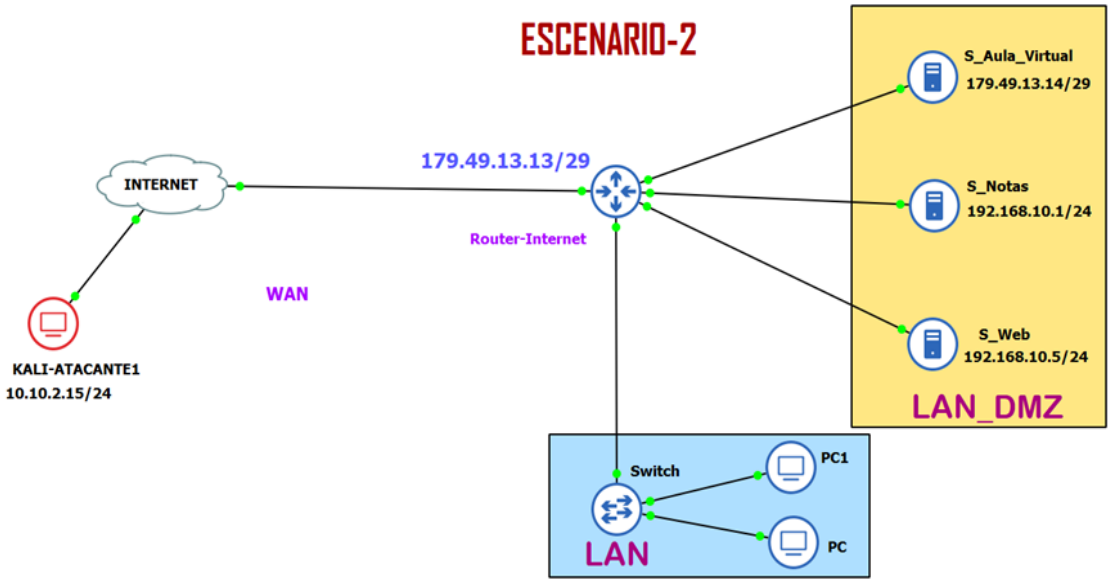
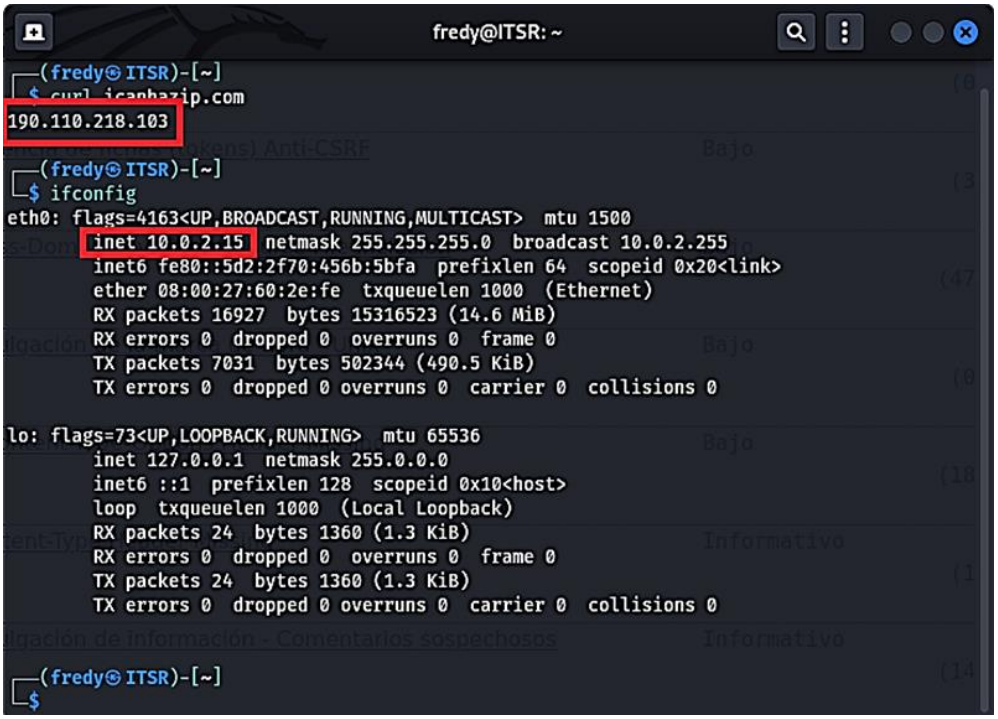


Figura 18-3: Diagrama del Escenario-2 para el Testing de análisis de vulnerabilidades.
Realizado por: Estrada Marco,2022

Para el Testing con el segundo escenario nos basamos en el diagrama mostrado en la Figura 18-3, en la cual el atacante es externo a la organización, es decir establecida por una red WAN, la cual tiene la dirección IP mostrada en la Figura 20-3



Mientras que el servidor web, al cual se realizará el Testing se encuentra con la dirección ip **179.49.13.14.,** tal y como se muestra en la Figura 19-3.

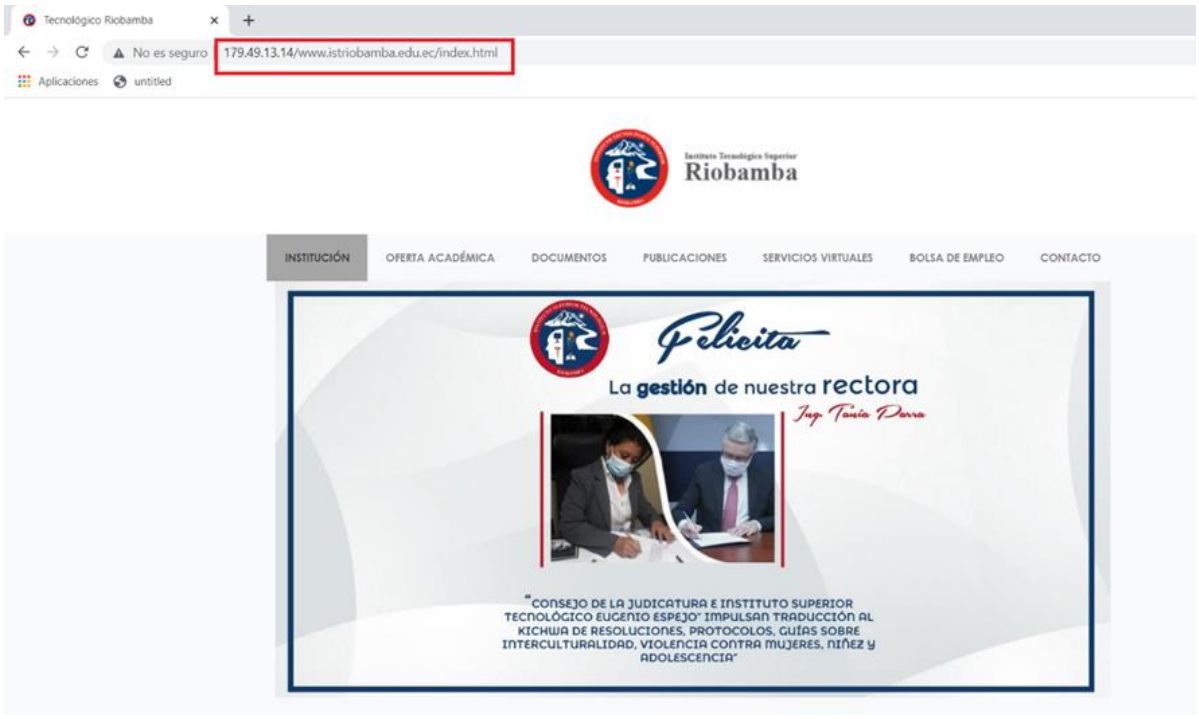


Figura 19-3: Dirección ip del servidor web del ISTR.
Realizado por: Estrada Marco,2022

Al mostrar la figura 20-3 se observa la conectividad entre el atacante y el servidor web.

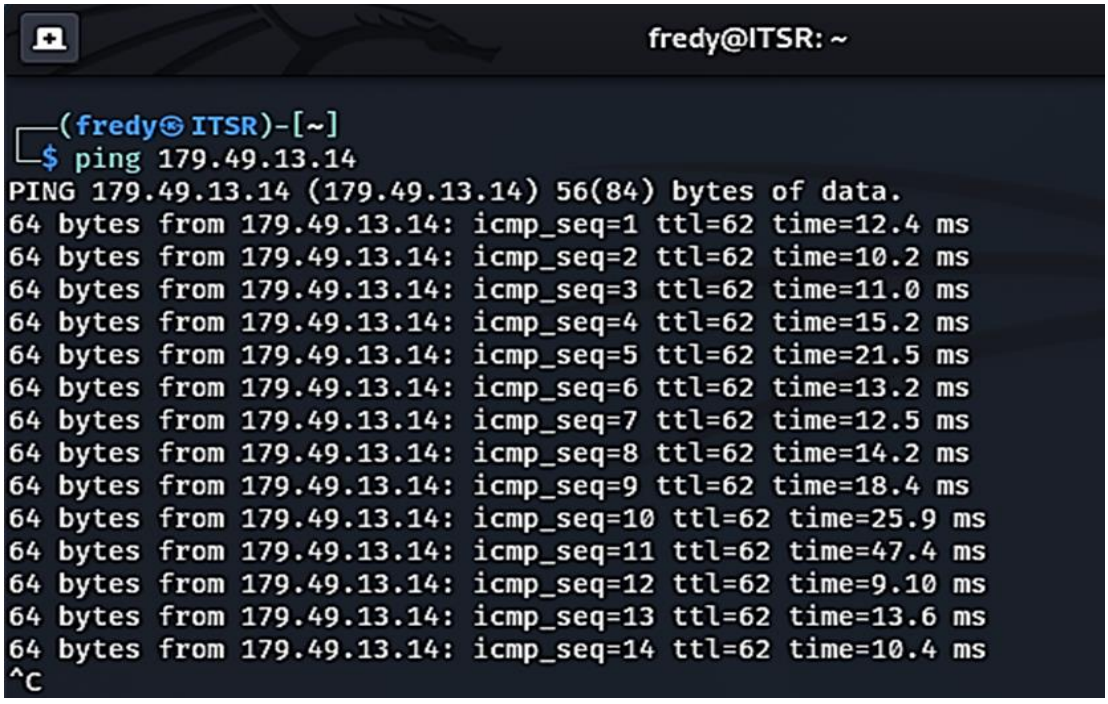


Figura 20-3: Verificación de conectividad, entre el Servidor y el atacante

Realizado por: Estrada Marco,2022

❖ **Testing con la herramienta NMAP**

Para el Testing con la herramienta NMAP, se usa el comando usado en el escenario 1, con la pretendemos conocer principalmente el OS, y los puertos que se encuentran habilitados. Donde una vez aplicado el escaneo se observa los resultados mostrados en la Figura 21-3 y Figura 22-3.

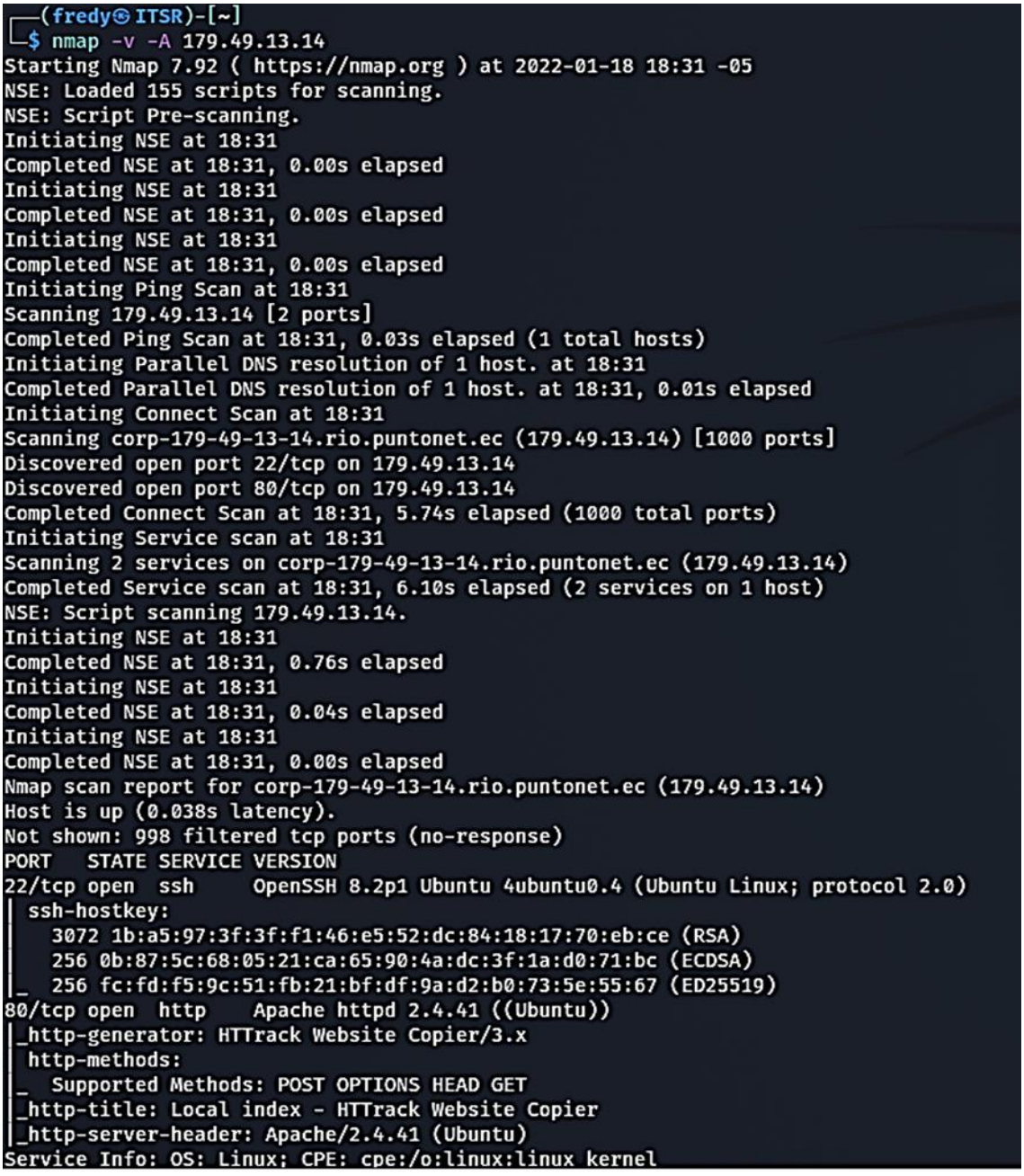


Figura 21-3: Resultado mediante Nmap, Escenario-2.

Realizado por: Estrada Marco,2022

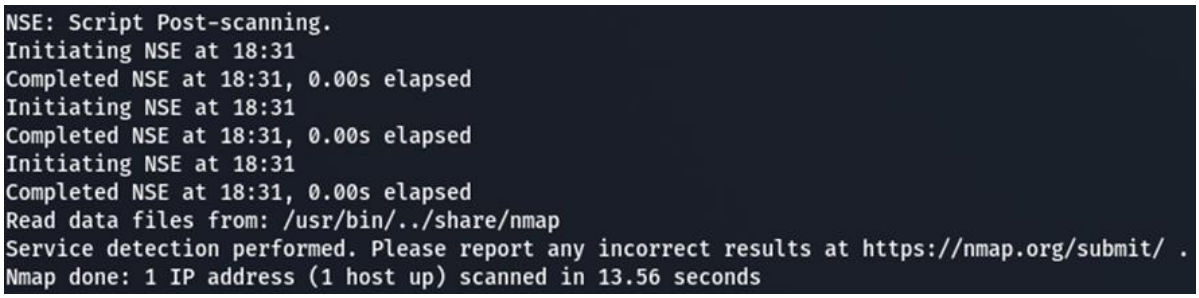


Figura 22-3: Resultados con Nmap, Escenario-2.

Realizado por: Estrada Marco,2022.

Una vez observada los resultados mostrados en las Figura 23-3 y Figura 24-3 se puede principalmente apreciar que se ha podido obtener los siguientes resultados:

- Los puertos habilitados son eel 22/tcp de ssh y el puerto 80/tcp de http.
- Cuenta con un OS: Linux.
- El servidor Web se encuentra montada en la distribución Ubuntu de Linux mediante Apache/2.4.41.
- El servidor Web tiene activo el servicio de SSH a través de OpenSSH versión: 8.2p1 y adicionalmente se pueden observar las llaves de encriptación que usa el servicio.
- También se puede apreciar que el servidor Web se encuentra clonada, mediante el generador Website HTTrack.

❖ **Testing con la herramienta OWASP**

Mediante la herramienta owasp, se pudo realizar un barrido total de las vulnerabilidades que puede presentar nuestro servidor Web, para la cual se adjunta a continuación las capturas más relevantes, en donde se muestra estadísticamente el nivel y la cantidad de vulnerabilidades existentes. Para lo cual, se muestra la puesta en escena mediante la Figura 23-3 el ataque a realizar mediante owasp.

Figura 23-3: Puesta en acción mediante Owaps, para el análisis de vulnerabilidad

Realizado por: Estrada Marco,2022.

Figura 24-3: Parámetros de reporte con Owaps.

Realizado por: Estrada Marco,2022.

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	Alto	Medio	Bajo	Total
Risk	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	0 (0,0 %)	0 (0,0 %)	399 (14,2 %)	0 (0,0 %)	399 (14,2 %)
	Bajo	0 (0,0 %)	0 (0,0 %)	1950 (69,2 %)	7 (0,2 %)	1957 (69,4 %)
	Informativo	0 (0,0 %)	0 (0,0 %)	440 (15,6 %)	22 (0,8 %)	462 (16,4 %)
	Total	0 (0,0 %)	0 (0,0 %)	2789 (99,0 %)	29 (1,0 %)	2818 (100%)

Figura 25-3: Estadísticas de alertas, obtenidas mediante Owasp.

Realizado por: Estrada Marco,2022.

A continuación, en la Figura 26-3, se puede conocer acerca de las alertas encontradas, y en el archivo adjunto sus posibles soluciones, que se deben realizar directamente al nivel de aplicación.

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medio	397 (14,1 %)
Vulnerable JS Library	Medio	2 (0,1 %)
Ausencia de fichas (tokens) Anti-CSRF	Bajo	96 (3,4 %)
Cross-Domain JavaScript Source File Inclusion	Bajo	1335 (47,4 %)
Divulgación de la marca de hora - Unix	Bajo	7 (0,2 %)
X-Content-Type-Options Header Missing	Bajo	519 (18,4 %)
Content-Type Header Missing	Informativo	46 (1,6 %)
Divulgación de información - Comentarios sospechosos	Informativo	416 (14,8 %)
Total		2818

Figura 26-3: Resumen de tipos de los tipos de alertas obtenidas con Owasp.

Realizado por: Estrada Marco,2022.

❖ **Testing con la herramienta Hping3 (DoS)**

Para la realización del ataque DoS, se realizó utilizando el modo flood (Ver Figura 29-3), donde una vez escaneada el puerto que se encuentra habilitada mediante Nmap (puerto 80), se pudo tener un ataque exitoso. Es importante mencionar que el ataque DoS, se logró tener éxito a los 12 min aproximadamente, las razones pueden ser varias, latencia (tiempo de respuesta), el ancho de banda de la red del atacante, o los recursos con los que la misma se maneje. A diferencia que al realizar un ataque localmente se pudo comprobar que se tuvo éxito aproximadamente a los 4 min de haber iniciado la inundación de paquetes, lo cual me da a entender que el servidor web no se encuentra a salvo, si un miembro de la organización, conocedora de la red por cualquiera de las razones tenga la mala voluntad de realizar un ataque DoS.

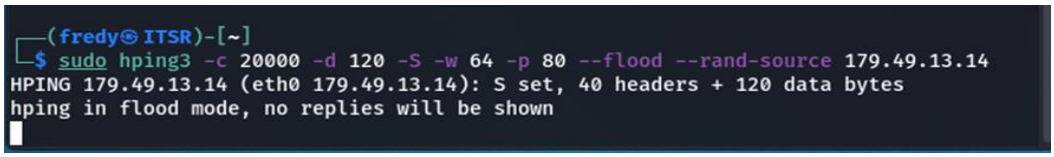


Figura 27-3: Ataque mediante Hping3 al servidor Web, Escenario-2.

Realizado por: Estrada Marco,2022.

Así mismo en la figura 28-3 se observa la comprobación de la denegación de servicio en el servidor web, pasado 12 min el ataque fue exitoso.

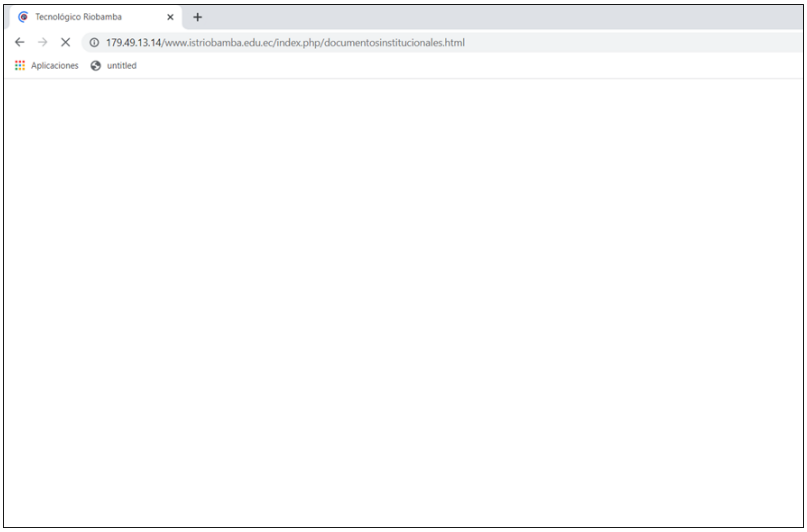


Figura 28-3: Ataque exitoso al servidor Web mediante Hpin3.

Realizado por: Estrada Marco,2022

Se logró el ataque de denegación de servicio al servidor web, con las siguientes estadísticas, tal y como se muestra en la Figura 29-3.

```
┌──(fredy㉿ITSR)-[~]
└─$ sudo hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 179.49.13.14
HPING 179.49.13.14 (eth0 179.49.13.14): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 179.49.13.14 hping statistic ---
20115977 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figura 29-3: Estadísticas del ataque ejecutado al servidor Web, mediante Hping3.

Realizado por: Estrada Marco,2022.

Y posteriormente a la verificación del ataque, se prosiguió a la cancelación de la inundación de paquetes, para levantar nuevamente el servidor Web, como podemos apreciar en la Figura 30-3.

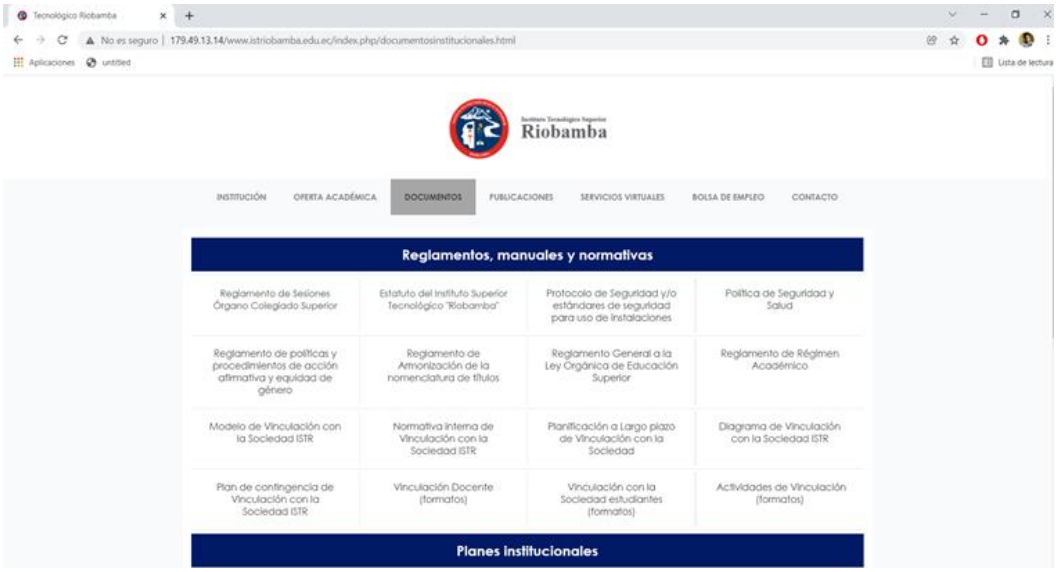


Figura 30-3: Restablecimiento del servidor Web, una vez cancelado el ataque con Hping3.

Realizado por: Estrada Marco,2022.

❖ Testing con la herramienta NIKTO

Mediante Nikto, se pudo recabar información acerca de todas las vulnerabilidades que el servidor Web presenta, tal y como se puede apreciar en la Figura 31-3.

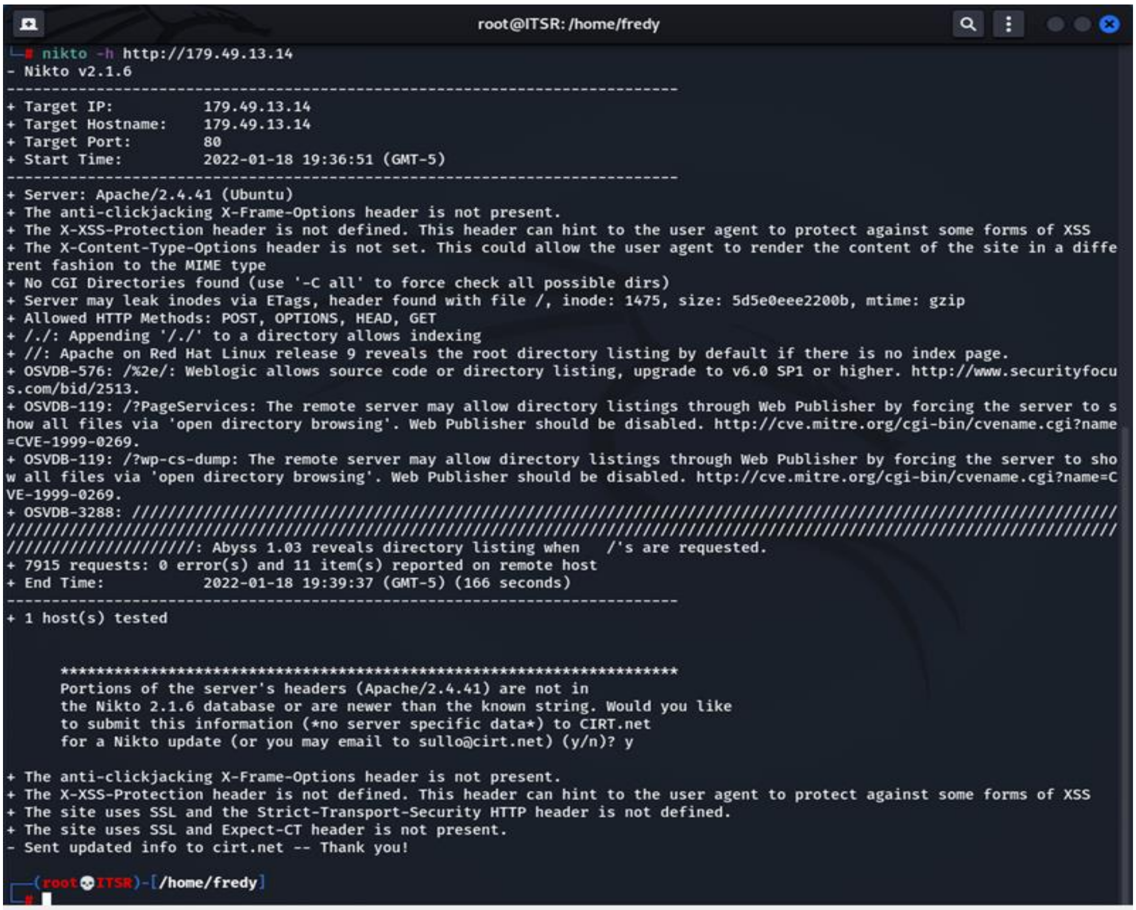


Figura 31-3: Ataque mediante la herramienta NIKTO.

Realizado por: Estrada Marco,2022.

Tanto en el escenario 1 y 2 al usar NIKTO, se ha podido coincidir encontrar las siguientes principales vulnerabilidades:

- X-Frame-Options anti-clickjacking no está presente
- X-XSS-Protection no está definido.
- X-Content-Type-Options no está configurado. Esto podría permitir que el agente de usuario represente el contenido del sitio de una manera diferente al tipo MIME.
- OSVDB-576 (CVE-2015-1476), permite mostrar la lista de directorios con sus contenidos, actualice a v6.0 SP1 o superior.

- OSVDB-119 (CVE-1999-0269), el servidor remoto puede permitir listados de directorios a través de Web Publisher obligando al servidor a mostrar todos los archivos a través de 'exploración de directorio abierto'. Web Publisher debe estar deshabilitado.

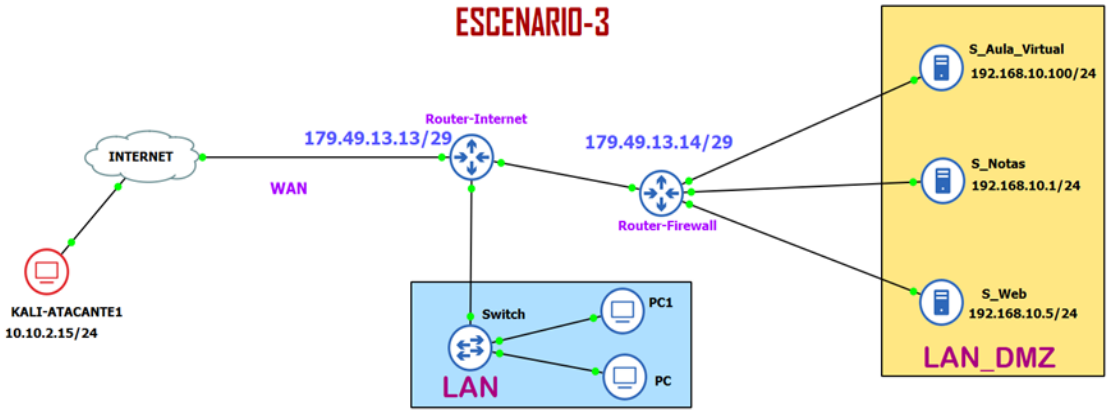


Figura 32-3: Diagrama del Escenario-3.

Realizado por: Estrada Marco,2022.

Para el escenario planteado en la Figura 32-3, el atacante al igual que en el escenario 2, será externo a la organización, perteneciente a una red wan, en donde se puede apreciar ya segmentada la red LAN_DMZ en donde se encuentra el servidor web, la cual directamente se encuentra conectada al Router Firewall que tiene la dirección 179.49.13.14 la cual será la IP pública en donde se mostrará el servidor Web y por ende por donde se realizará el ataque. En cuanto al servidor tendrá una dirección local, y esta será nateada con el router firewall para su salida a internet, en la Figura 33-3 se muestra la dirección IP, del atacante.

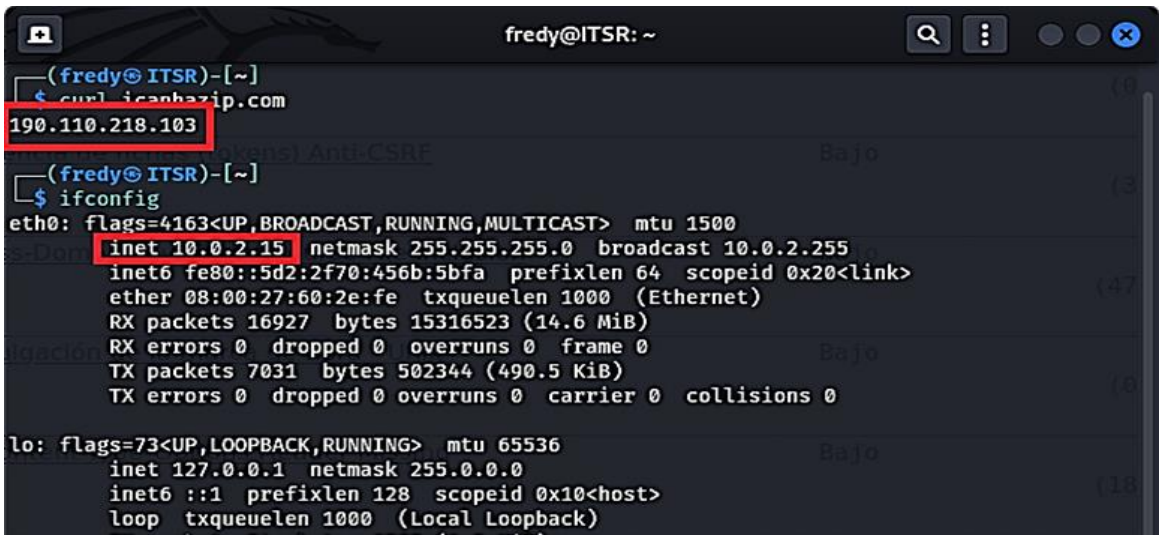


Figura 33-3: Dirección Ip del atacante.

Realizado por: Estrada Marco,2022

Por otro lado, el servidor Web, tendrá la dirección **IP: 179.49.13.14,** la cual se puede apreciar en la Figura 34-3

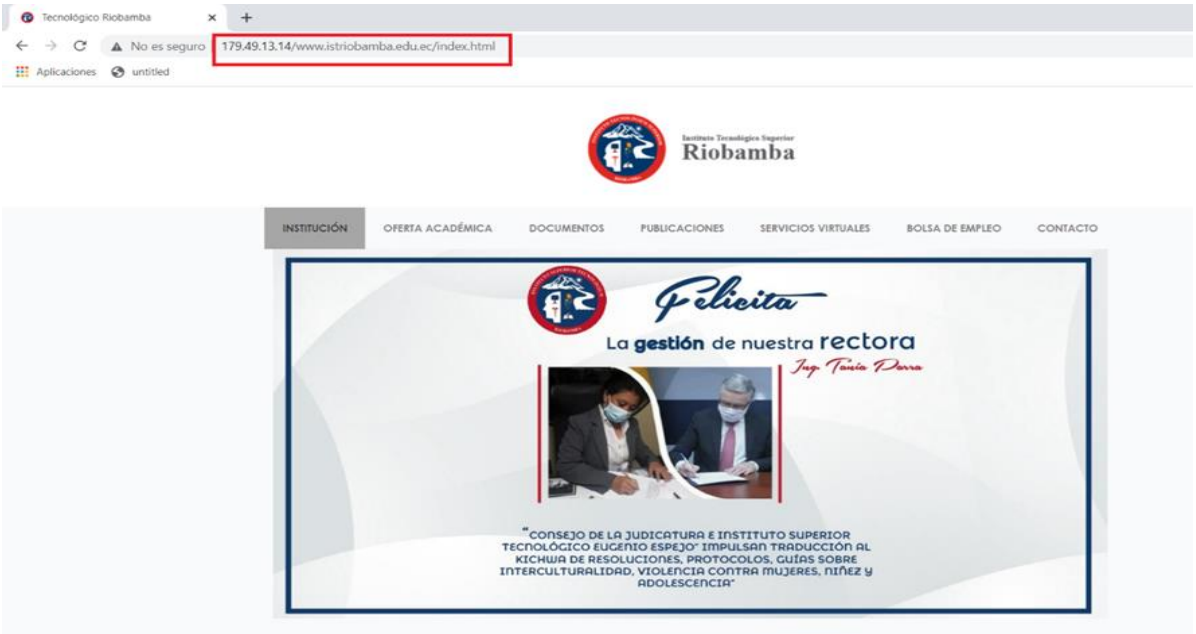


Figura 34-3: Dirección del servidor Web

Realizado por: Estrada Marco,2022

Se verifica la conectividad, entre el atacante y el servidor web a atacar, mediante ping, tal y como podemos observar en la Figura 35-3

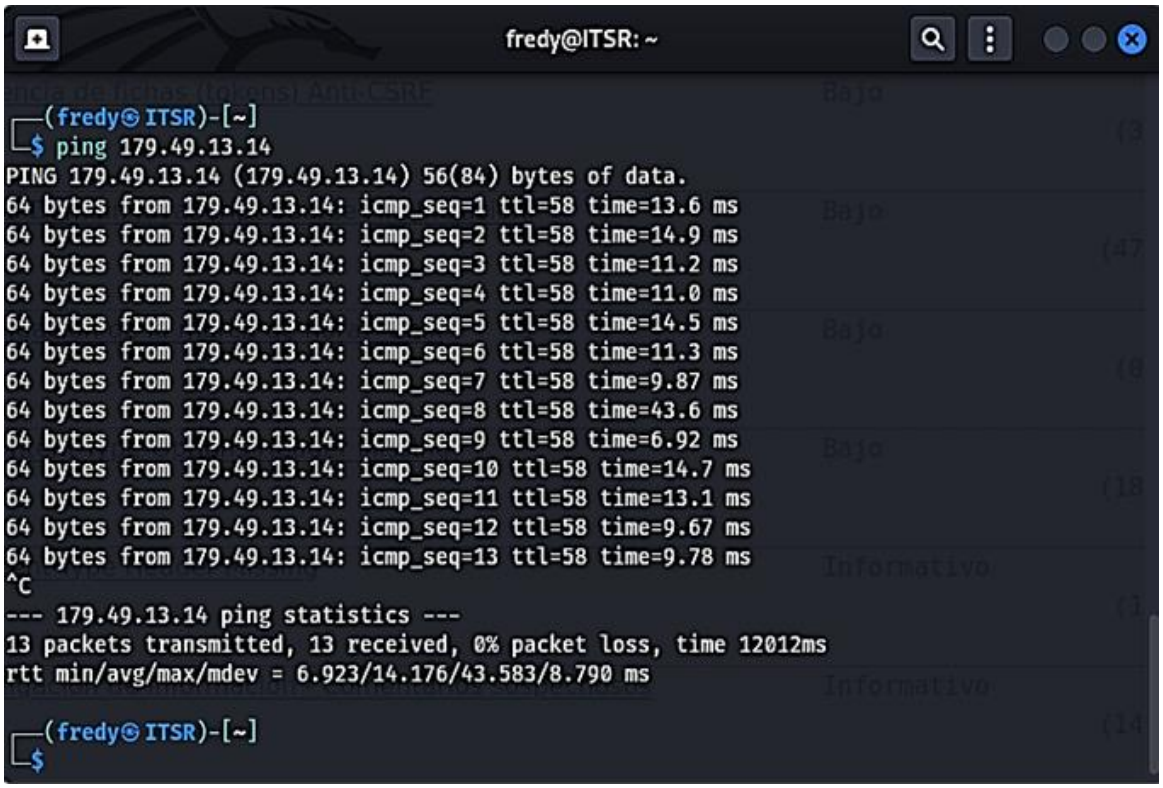


Figura 35-3: Verificación de conectividad entre el Servidor y el atacante.

Realizado por: Estrada Marco,2022

Se puede apreciar en la Figura 36-3 el direccionamiento, en donde la LAN DMZ se encuentra en conectividad por el ether 4.

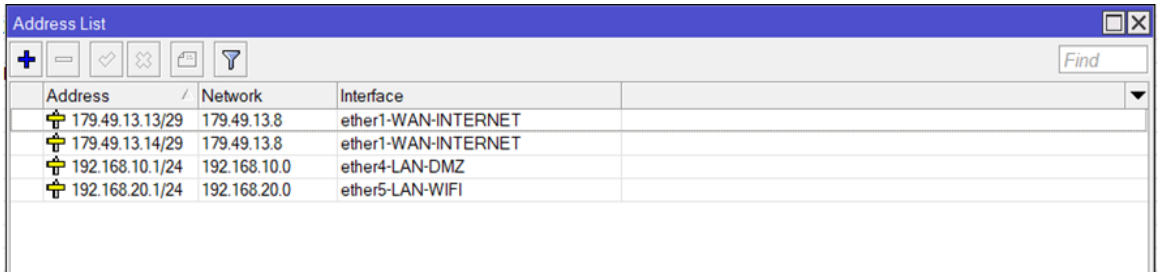


Figura 36-3: Direccionamiento ip del Rio_Firewall_01.

Realizado por: Estrada Marco,2022

Así como también en el firewall se tiene realizada el Nateo como se puede apreciar en la Fig. 37-3.

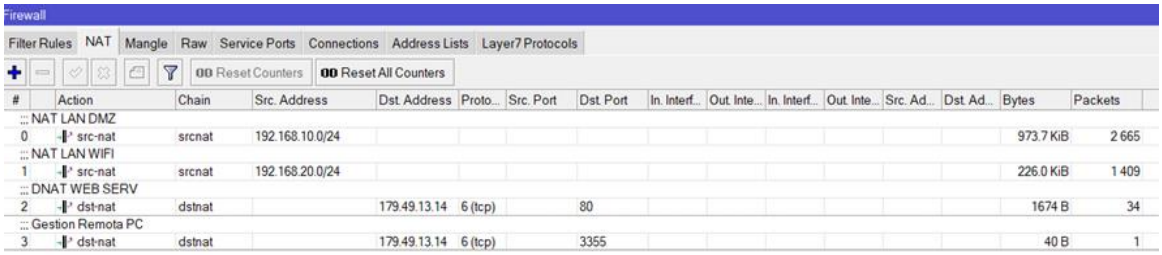


Figura 37-3: Reglas de NAT en RIO_FIREWALL_01

Realizado por: Estrada Marco,2021

En la Fig. 38-3 se puede apreciar la lista de las conexiones del DHCP server, en la cual me muestra detalladamente las direcciones conectadas, junto a ella la información de su MAC Address y el nombre del host, entre las características principales

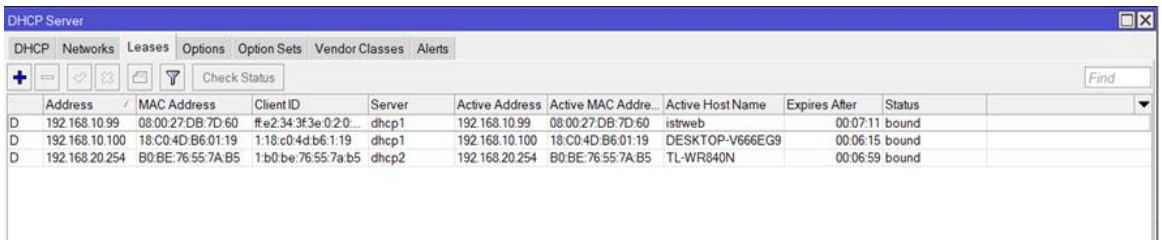


Figura 38-3: DHCP Server de RIO_FIREWALL_01

Realizado por: Estrada Marco,2021

Las reglas que se encuentran presente en el firewall son las siguientes mostradas en la Fig. 39-3.

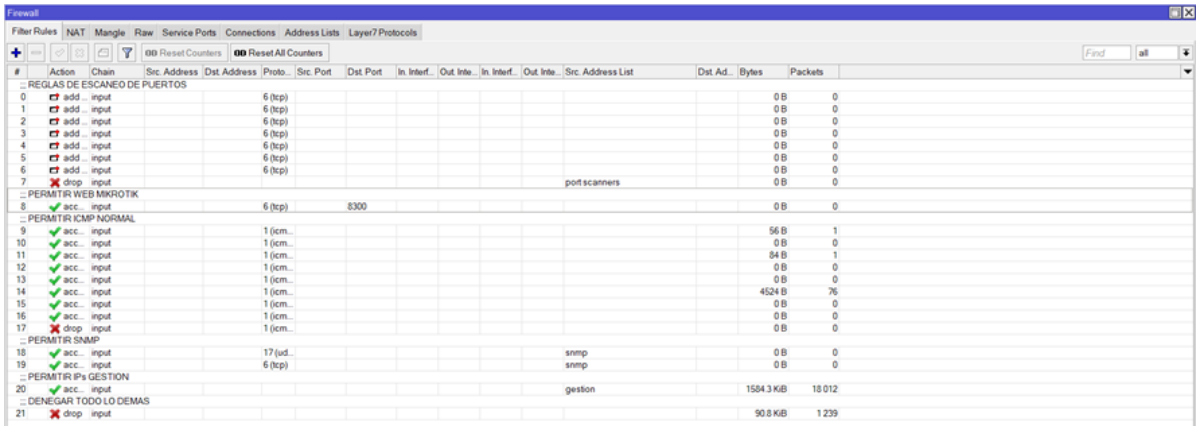


Figura 39-3: Reglas de Firewall en RIO_FIREWALL_01

Realizado por: Estrada Marco,2022

3.7.3 Fase 3. Generación de informes

Una vez descubiertas las amenazas y vulnerabilidades realizadas en las fases uno y dos, se establece las correcciones específicas para los dos posibles escenarios donde puedan existir intrusos en la red, con la herramienta Owasp top 10 encontramos 10 vulnerabilidades, pero se tomará en cuenta 7 más significativas.

Para lograr la seguridad, la confidencialidad y que la plataforma académica del Instituto Superior Tecnológico Riobamba sea robusta se crean políticas de seguridad, realizando un informe con términos técnicos y comunes para que todas las personas que usen la plataforma académica puedan conocer, mejorar la cultura de prevención contra ataques de externos o personas que no tienen nada que ver con el uso de la plataforma académica. En el siguiente capítulo se redacta la implementación de seguridades en la red para cumplir los objetivos de la investigación.

CAPÍTULO IV

4 RESULTADOS Y DISCUSIÓN

4.1 Presentación de resultados

Este capítulo muestra los resultados obtenidos en la investigación realizada, a través del uso de la metodología mencionada anteriormente.

4.2 Resultados de la fase 1-Recopilación de la información

En la siguiente tabla 4-4 muestra los dispositivos y equipos informáticos con los que cuenta la plataforma académica del Instituto Superior Tecnológico Riobamba, conociendo la infraestructura y funcionamiento de esta, también implementando el firewall a la red mejorando la seguridad del tráfico de datos en la red.

Tabla4-4: Listado de dispositivos de la plataforma informática

DISPOSITIVO	FUNCIONAMIENTO
Página web	Página oficial donde se puede seleccionar los diferentes servicios que ofrece el Instituto Superior Tecnológico Riobamba. www.istriobamba.edu.ec
Servidor Base de Datos	Servidor de base de datos donde se almacena la información histórica y actual del personal docente, administrativo y estudiantes, MySQL sistema operativo CENTOS IP: 174.24.10.3/24
Servidor Aplicativo Web	Servidor que maneja el aplicativo de calificaciones donde tienen permiso de ingreso estudiantes, alumnos y autoridades, Sistema Operativo: Windows Server IP: http://174.24.10.2:9696/VenusIESJsp/inicio.jsp
Servidor Moodle	Servidor que maneja plataformas académicas donde tienen permiso de ingreso estudiantes y docentes, Sistema Operativo: Ubunto IP: http://174.24.10.4/moodle/.php
Servidor aplicativo biblioteca	Servidor que maneja el aplicativo de biblioteca teniendo permiso, personal encargado, estudiantes y docentes, Sistema Operativo: Windows Server, IP:http://www.bibliotecaistriobamba.com/
Firewall WAN	La marca que se adquirió para este proyecto es MIKROTIK su principal función es administrar el servicio de internet permitiendo el paso de los usuarios que se conectan a los diferentes servicios que ofrece la plataforma académica.
Firewall LAN	La marca utilizada es Mikrotik, su principal función es generar reglas y evitar que usuarios realicen malas prácticas dentro de la plataforma.

Fuente: (Espinoza, 2019)

Realizado por: Marco Estrada. 2022

4.3 Resultados de la fase 2- Análisis y explotación de vulnerabilidades

Con la ayuda de la herramienta Owasp Top 10 se comprobó que el aplicativo web del Instituto Superior Tecnológico Riobamba tiene varias debilidades como se muestra en la siguiente lista:

- Application Error Disclosure (Divulgación de error de aplicación). - revela información confidencial, como la ubicación del archivo que produjo la excepción.
- Exploración de Directorios. - proporciona directorios y archivos disponibles a través de una dirección URL.
- Missing Anti-clickjacking header (Falta de encabezado clickjacking) esta opción no protege de los ataques clickjacking
- Vulnerable JS Library (Vulnerabilidad JS). - vulnerabilidades en programación Java Script
- Cross-Domain JavaScript Source File Inclusion (inclusión de archivos fuente) este error tiene la característica de fugar información confidencial como datos personales.
- X-Content-Type-Options Header missing (falta contenido tipo X). - error que indica contenido distinto al programado
- Divulgación de información-Comentarios sospechosos.

Al momento de encontrar 7 de las 10 vulnerabilidades a través del programa OWASP TOP 10 nos percatamos que todas pueden ser controladas y prevenidas.

4.4 Resultados de indicadores

Con el escaneo de las vulnerabilidades y amenazas al sistema institucional nos damos cuenta de que reduce los riesgos aplicando el plan de seguridad anti phising utilizando un firewall propuesto en la investigación. Las dos opciones que no controla son las que encontramos en la siguiente tabla:

Tabla 5-4: Descripción de vulnerabilidades que no se pueden descartar

Vulnerabilidad Detectadas con OWASP	Descripción
A3.-Missing Anti-clickjacking header	No incluye en la política de seguridad de un firewall recomendable que se adquiera un certificado de seguridad
A6.- X-Content-Type-Options Header missing	No incluye en la política de seguridad ya que depende del usuario final que tenga actualizado su navegador de internet.

Fuente: (Espinoza, 2019)

Realizado por: Marco Estrada. 2022

Utilizando el plan de seguridad anti-phishing utilizando un firewall en la plataforma informática del Instituto Superior Tecnológico Riobamba cumple satisfactoriamente los objetivos. En la figura 41-4 comprobamos de forma gráfica la mejora de seguridad, menorando las vulnerabilidades encontradas.

Tabla 6-4: Minimización de vulnerabilidades que se encontraron en la plataforma institucional

Parámetro para evaluar	**Vulnerabilidad encontrada**	**Vulnerabilidad de la Plataforma Institucional**
Plataforma institucional sin sistema de seguridad antiphishing	7	100%
Plataforma institucional con sistema de seguridad antiphishing	2	28.5%

Fuente: (Espinoza, 2019)

Realizado por: Marco Estrada. 2022

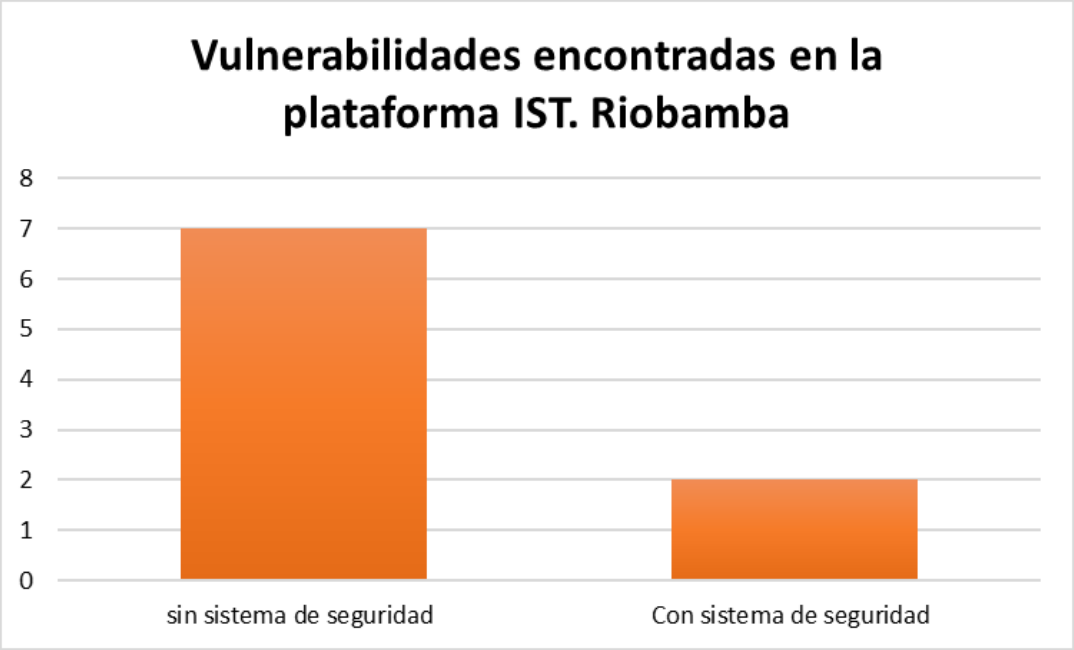


Figura 1-4: Número de Vulnerabilidades encontradas en la plataforma Institucional

Realizado por: Estrada Marco,2022

4.4.1 Análisis e interpretación de los resultados

Con los datos encontrados realizando la aplicando la herramienta owasp top 10 en la plataforma institucional nos indica que 7 son las vulnerabilidades correspondiente eso al 100% dentro del escenario sin utilizar el plan de seguridad anti phishing, mientras que cuando se aplica el sistema de seguridad a través de un firewall se obtiene 2 vulnerabilidades con un porcentaje de 28%, deduciendo que cuando se aplica el sistema de seguridad mejora su nivel de seguridad casi en un 72.2% de toda la plataforma institucional del IST. Riobamba.

4.5 Prueba de la hipótesis de investigación

Con los resultados obtenidos en el capítulo 3 de esta investigación se comprueba el nivel de seguridad como se encontraba antes de esta investigación y como mejora con la implementación del sistema de seguridad anti-phishing protegiendo la información utilizando un firewall. Se utilizaron 3 escenarios para realizar las pruebas y comprobar si el sistema de seguridad en la plataforma del Instituto Superior Tecnológico Riobamba se encuentra correctamente funcionando.

Las consideraciones que se tomaron en cuenta para las pruebas se muestran en la siguiente tabla:

Tabla 7-4: Consideraciones para las pruebas en la plataforma del Instituto Superior Tecnológico Riobamba

ESCENARIO 1	● Plataforma Institucional del IST. Riobamba en funcionamiento. ● Análisis de un ataque dentro de la Red LAN donde están todos los servidores conectados. ● Owasp top 10 evaluando las vulnerabilidades.
ESCENARIO 2	● Plataforma Institucional del IST. Riobamba en funcionamiento. ● Análisis de un ataque a la Red Institucional a través del Internet (RED WAN) ● Owasp top 10 evaluando las vulnerabilidades.
ESCENARIO 3	● Plataforma Institucional del IST. Riobamba en funcionamiento. ● Owasp top 10 evaluando las vulnerabilidades. ● Se implementó un Firewall conectado en la red LAN para su seguridad de la información que poseen los servidores.

Fuente: (Espinoza, 2019)

Realizado por: Marco Estrada. 2022

Para la comprobación de la hipótesis se tomará al escenario 1 y 2 como uno solo refiriéndonos a que no posee el sistema de seguridad anti-phishing y el escenario 3 tiene se implementó el firewall que es nuestro escenario para comprobar la hipótesis.

4.5.1 Valoración de la variable independiente

La variable independiente es el "Sistema de Seguridad anti-phishing utilizando un Firewall." como técnica de aprobación se utilizó la observación validando los requerimientos planteados para la evaluación de vulnerabilidades en el escenario institucional.

4.5.1.1 Indicador: Seguridad del sistema institucional

Para comprobar la seguridad se tomó en cuenta el listado de riesgos críticos indicados por la herramienta OWASP Top 10 aplicados a la red institucional, se seleccionó las vulnerabilidades que son más representativas para el funcionamiento de toda la red para el presente estudio como se muestra en la siguiente tabla.

Tabla 8-4: Vulnerabilidades detectadas en la plataforma Institucional

Vulnerabilidad Detectadas con OWASP
A1.- Application Error Disclosure
A2.- Exploración de Directorios
A3.-Missing Anti-clickjacking header
A4.- Vulnerable JS Library
A5.- Cross-Domain JavaScript Source File Inclusion
A6.- X-Content-Type-Options Header missing
A7.- Divulgación de información-Comentarios Sospechosos

Fuente: (Espinoza, 2019)

Realizado por: Marco Estrada. 2022

4.5.2 Valoración de variable dependiente

Para la valoración de las "Amenazas y fallas del sistema de seguridad en la plataforma institucional" se utilizó varias herramientas de Kali Linux, para comprobar la estabilidad del sistema entre ellas: NMAP, NIKTO, HPING3, OWASP.

4.5.2.1 Indicador: Número de Amenazas a la red encontrada.

Utilizando varias herramientas para detectar y explotar las vulnerabilidades en la plataforma institucional comprobamos lo siguiente:

Tabla 9-4: Análisis de vulnerabilidades detectadas en la plataforma Institucional con y sin sistema de seguridad

Vulnerabilidad Detectadas con OWASP	Sin el Sistema de Seguridad Anti-phishing	Con el Sistema de Seguridad Anti-phishing utilizando un firewall
A1.- Application Error Disclosure	X	
A2.- Exploración de Directorios	X	
A3.-Missing Anti-clickjacking header	X	X
A4.- Vulnerable JS Library	X	
A5.- Cross-Domain JavaScript Source File Inclusion	X	
A6.- X-Content-Type-Options Header missing	X	X
A7.- Divulgación de información-Comentarios Sospechosos	X	
Total	7	2

Fuente: (Pinango, 2021)

Realizado por: Marco Estrada. 2022

4. 6 Comprobación estadística de la hipótesis

En la comprobación de la hipótesis general "La implementación de un sistema de seguridad anti-phishing con firewall mediante software libre mejorará la integridad y confidencialidad de la información en los sistemas en línea", se utilizó la prueba estadística del Chi-Cuadrado (2).
Definiendo a la Hipótesis de Investigación (Hi) y la Hipótesis Nula (Ho):

Hi: La implementación de un sistema de seguridad anti-phishing con firewall en la plataforma informática mejorará la integridad y la confidencialidad de la información del Instituto Superior Tecnológico Riobamba.

Ho: La implementación de un sistema de seguridad anti-phishing con firewall en la plataforma informática **no** mejorará la integridad y la confidencialidad de la información del Instituto Superior Tecnológico Riobamba.

Para comprobar la hipótesis se presenta la siguiente tabla donde constan las frecuencias encontradas en la investigación.

Tabla10-4: Tabla de frecuencias con cantidades exploradas

Variables para evaluar	Escenario 1 (Plataforma institucional sin sistema de seguridad anti phishing)	Escenario 2 Plataforma institucional con sistema de seguridad anti phishing	Total
Vulnerabilidades encontradas	7	2	9
Vulnerabilidades resueltas	0	5	5
Total	7	7	14

Fuente: (Pinango, 2021)

Realizado por: Marco Estrada. 2022

Es necesario aplicar la siguiente fórmula para obtener la frecuencia esperada de la tabla.

$$Fe = \frac{(total\ columna\ \times total\ fila)}{Suma\ total}$$

Tabla 11-4: Tabla con valores de frecuencias esperadas

Variables para evaluar	Escenario 1 (Plataforma institucional sin sistema de seguridad antiphishing)	Escenario 2 Plataforma institucional con sistema de seguridad antiphishing	Total
Vulnerabilidades encontradas	4.5	4.5	9
Vulnerabilidades resueltas	2.5	2.5	5
Total	7	7	14

Fuente: (Pinango, 2021)

Realizado por: Marco Estrada. 2022

Es necesario aplicar la siguiente fórmula para obtener la frecuencia esperada de la tabla.

$$Fe = \frac{(total\ columna\ \times total\ fila)}{Suma\ total}$$

Tabla 12-4: Tabla con valores de frecuencias esperadas

Variables a evaluar	Escenario 1 (Plataforma institucional sin sistema de seguridad antiphishing)	Escenario 2 Plataforma institucional con sistema de seguridad antiphishing	Total
Vulnerabilidades encontradas	4.5	4.5	9
Vulnerabilidades resueltas	2.5	2.5	5
Total	7	7	14

Fuente: (Pinango, 2021)

Realizado por: Marco Estrada. 2022

Después, se calcula el valor de Chi- cuadrado mediante la siguiente fórmula:

$$x^2 = \sum \frac{(FO - FE)^2}{FE}$$

Dónde:

F0: Frecuencia observada en cada celda

FE: Frecuencia esperada en cada celda

$$X^2 = \frac{(7\text{-}4.5)^2}{4.5} + \frac{(0\text{-}2.5)^2}{2.5} + \frac{(2\text{-}4.5)^2}{4.5} + \frac{(5\text{-}4.5)^2}{2.5}$$

$$x^2 = 5.377$$

Para seguir con el cálculo necesitamos conocer los grados de libertad para aplicar el chi cuadrado utilizaremos la siguiente fórmula.

$$\boldsymbol{v} = (r - 1) * (k - 1)$$

Dónde:

r: es el número de filas

k: es el número de columnas

$$\boldsymbol{v} = (2-1) * (2-1)$$

$$\boldsymbol{v} = 1$$

Con lo obtenido en los cálculos anteriores, determinamos que el grado de significancia sera de 0.1% obteniendo el punto crítico con un grado de libertad de 1.

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

Figura 2-4: Tabla de distribución estadística de Chi Cuadrado

Realizado por: Marco Estrada. 2022

Con los resultados obtenidos H0 debe ser aceptada si sucede lo siguiente

$$\boldsymbol{x^2 calculado \leq x^2 crítico}$$

Si no se cumple se rechaza H0 y se acepta Hi

Los resultados son los siguientes

$$\boldsymbol{x^2 calculado} = 5.377$$

$$\boldsymbol{x^2 crítico} = 3.8415$$

Para poder emitir algún criterio de decisión utilizaremos el siguiente gráfico.

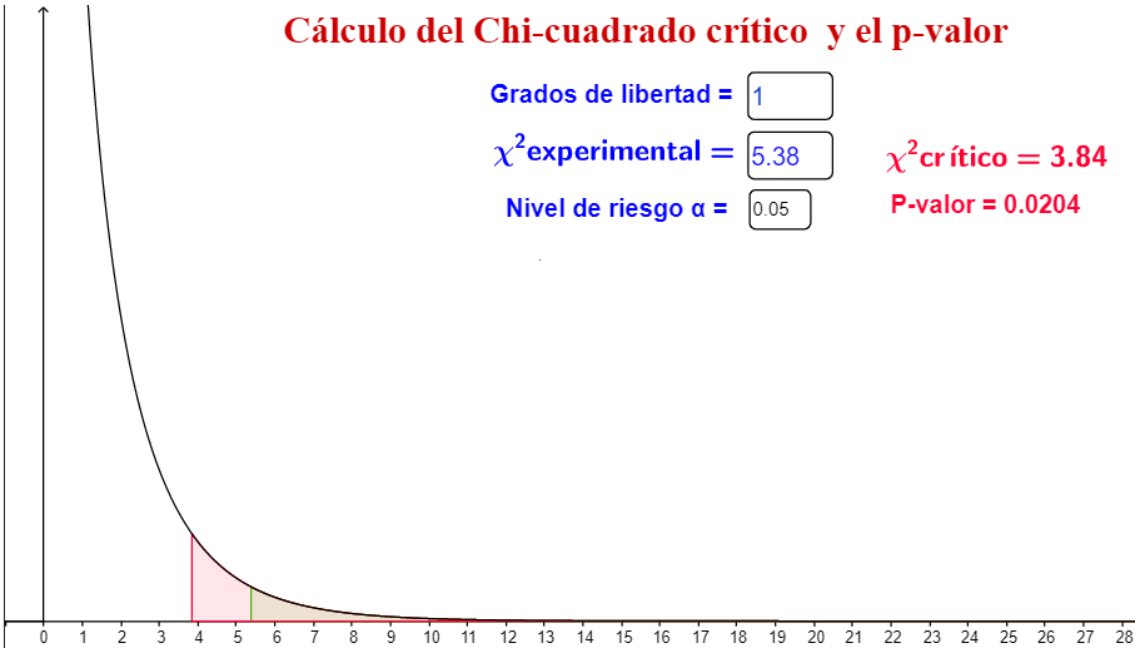


Gráfico 1-4: Chi-Cuadrado y criterios de aceptación de Hi

Elaborado por: Estrada Marco,2022

4.7 Interpretación y análisis

Con los resultados obtenidos y como se puede observar en la gráfica se propone rechazar la Hipótesis nula (H0) aceptando la hipótesis alternativa (Hi) teniendo un nivel de confianza del 95% y 5% de nivel de significancia.

CAPÍTULO V

5. PROPUESTA

Conociendo que la seguridad informática es muy importante en toda organización principalmente cuando los datos o la información que guarda es muy dedicada, y se presenta a temas de fomentar culturas para prevenir robos modificación de datos, utilizando para esto un sistema de seguridad anti phishing.

Este capítulo se enfoca a mostrar la programación que se realizó en el firewall para evitar el mal uso de la plataforma académica del Instituto Superior Tecnológico Riobamba evitando el paso de personas que realizan varios procesos extraños a los comunes y habituales.

5.1 Sistema de seguridad anti phishing utilizando un firewall

5.1.1 Objetivo

Poseer estrategias programadas para evitar intrusos en los sistemas académicos del Instituto Superior Tecnológico Riobamba, de esta forma se tendrá seguridades de acceso para solo el personal involucrado directamente en los diferentes procesos que cuenta la institución.

5.1.2 Alcance

El sistema de seguridad anti phishing está diseñado para la plataforma institucional del Instituto Superior Tecnológico Riobamba ubicado en la ciudad del mismo nombre en la Av. Lizarzaburu y Av. La Prensa S/N dentro de la Unidad Educativa Riobamba.

El buen funcionamiento del sistema dependerá también de los administradores del área de las Tics del crecimiento de los servicios que brinda el instituto y del mantenimiento oportuno que se brinde al firewall, tendrá un gran alcance principalmente a la ciudadanía que confía y apuesta por la institución de educación superior.

5.1.3 Programación del Firewall contra intrusos en la red

A continuación, se da a conocer, las configuraciones de programación realizadas en el **RIO_FIREWALL_01**

En el presente apartado se asigna para cada una de las interfaces usadas un nombre de identificación, tal y como se puede apreciar en cada interfaz. Donde para la salida a internet se encuentra asignada la interfaz ether1, para la LAN_DMZ donde se encuentra el servidor Web se encuentra asignada el ether2 y finalmente para el ether3, 4, y 5 se encuentra asignada para conexiones locales.

/interface ethernet

set [find default-name=ether1] name=ether1-WAN-INTERNET

set [find default-name=ether2] name=ether2-DMZ

set [find default-name=ether3] name=ether3-LAN

set [find default-name=ether4] name=ether4-LAN

set [find default-name=ether5] name=ether5-LAN

En el presente apartado se configura un rango de pool de direcciones para la LAN de dhcp server, del Router-Firewall la misma que va desde la 192.168.20.2-192.168.20.254

/ip pool

add name=dhcp_pool1 ranges=192.168.20.2-192.168.20.254

/ip dhcp-server

add address-pool=dhcp_pool1 disabled=no interface=bridge-LAN name=dhcp1

/ip pool

add name=dhcp_pool0 next-pool=dhcp_pool0 ranges=192.168.30.2-192.168.30.10

En el presente apartado se configura la interfaz para la conectividad de una vpn, la cual se realizará se encuentra habilitada, todas las autentificaciones existentes: pap,chap,mschap1,mschap2.

/interface pptp-server server

set authentication=pap,chap,mschap1,mschap2 keepalive-timeout=disabled

En el presente apartado es importante resaltar la dirección WAN que permitirá al Router-Firewall salir a internet, mostrando el servidor Web, la cual se encuentra en la interfaz ether1, con la dirección 179.49.13.14/29

/ip address

add address=192.168.10.1/24 interface=ether2-DMZ network=192.168.10.0

add address=179.49.13.13/29 interface=ether1-WAN-INTERNET network=179.49.13.8

add address=179.49.13.14/29 interface=ether1-WAN-INTERNET network=179.49.13.8

add address=192.168.20.1/24 interface=bridge-LAN network=192.168.20.0

En el presente apartado perteneciente a la configuración de las direcciones del address-list en IP-FIREWALL de Rio_Firewall_01, se considera las direcciones de gestión DMZ y la dirección asignada para la gestión pública.

/ip dhcp-server network

add address=192.168.20.0/24 dns-server=8.8.8.8,8.8.4.4 gateway=192.168.20.1

/ip firewall address-list

add address=192.168.10.0/24 comment="Gestion DMZ" list=gestion

add address=179.49.13.8/29 comment="Gestion Publicas" list=gestion

/ip firewall filter

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input comment="REGLAS DE ESCANEO DE PUERTOS" protocol=tcp psd=21,3s,3,1

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=fin,syn

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=syn,rst

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg

add action=drop chain=input protocol=tcp psd=1,3s,3,1

add action=accept chain=input comment="PERMITIR WEB MIKROTIK" dst-port=8300 protocol=tcp

add action=accept chain=input comment="PERMITIR ICMP NORMAL" icmp-options=0:0 protocol=icmp

add action=accept chain=input icmp-options=3:0 protocol=icmp

add action=accept chain=input icmp-options=3:1 protocol=icmp

add action=accept chain=input icmp-options=3:4 protocol=icmp

add action=accept chain=input icmp-options=4:0 protocol=icmp

add action=accept chain=input icmp-options=8:0 protocol=icmp

add action=accept chain=input icmp-options=11:0 protocol=icmp

add action=accept chain=input icmp-options=12:0 protocol=icmp

add action=drop chain=input protocol=icmp

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=none-dynamic chain=input connection-limit=100,32 connection-nat-state=dstnat dst-address=179.49.13.14 \

dst-port=80 protocol=tcp

add action=drop chain=input connection-limit=10,32 connection-nat-state=dstnat dst-address=179.49.13.14 dst-port=80 protocol=tcp src-address-list="port scanners"

add action=accept chain=input comment="PERMITIR SNMP" port=161,162 protocol=udp src-address-list=snmp

add action=accept chain=input port=161,162 protocol=tcp src-address-list=snmp

add action=accept chain=input comment="PERMITIR IPs GESTION" src-address-list=gestion

add action=drop chain=input comment="DENEGAR TODO LO DEMAS" psd=5,3s,3,1

En el presente apartado perteneciente al NAT, del aparatado del firewall de Rio_Firewall_01 se realiza la traducción de direcciones de red, en donde es muy importante denotar que para el servidor web se lo realiza mediante el protocolo TCP y el puerto 80, en la cual la dirección local del servidor web es decir la que se encuentra dentro de la LAN_DMZ con la dirección de 192.168.10.5 tendrá un destino de nateo con la dirección 179.49.13.14, la cual le permitirá salir a internet y mostrarse mediante tal dirección. Es decir, una vez que se realice que el atacante intente vulnerar el servidor, en esta vez, tendrá que pasar por el router-firewall, la cual tendrá la misión de disminuir o mitigar los riesgos de ataques que se pueden presentar.

/ip firewall nat

add action=src-nat chain=srcnat comment="NAT LAN DMZ" src-address=192.168.10.0/24 to-addresses=179.49.13.14

add action=src-nat chain=srcnat comment="NAT LAN WIFI" src-address=192.168.20.0/24 to-addresses=179.49.13.13

add action=src-nat chain=srcnat comment="NAT VPN" src-address=192.168.30.0/24 to-addresses=179.49.13.13

add action=dst-nat chain=dstnat comment="DNAT WEB SERV" dst-address=179.49.13.14 dst-port=80 protocol=tcp to-addresses=192.168.10.5 to-ports=80

En el presente apartado podemos apreciar los servicios asignados por el firewall que pueden ser gestionados (Que se encuentran deshabilitados), en donde una vez que no se encuentre habilitada el tipo del servicio, el firewall hará caso omiso a las conexiones que intenten hacer adyacencia con esta. Podemos apreciar los servicios de:

/ip firewall service-port

set ftp disabled=yes

set tftp disabled=yes

set irc disabled=yes

set h323 disabled=yes

set sip disabled=yes

set pptp disabled=yes

set udplite disabled=yes

set dccp disabled=yes

set sctp disabled=yes

Se ha establecida una ruta estática, la cual tiene su salida o Gateway con la dirección 179.49.13.9

/ip route

add distance=1 gateway=179.49.13.9

En el presente apartado del RouterOs se puede apreciar que los siguientes servicios se encuentran deshabilitados:

- Telnet: protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.
- Ftp: Protocolo de transferencia de archivos.
- Ssh: Protocolo, cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.
- Api: Interfaz de programa de aplicaciones.

/ip service

set telnet disabled=yes

set ftp disabled=yes

set ssh disabled=yes

set api disabled=yes

set api-ssl disabled=yes

En el presente apartado se muestra a detalle la configuración de una vpn realizada, en donde se especifica la dirección local, el pool de direcciones y el tipo de encriptación usada. Así como también se puede apreciar el perfil creado por la persona que dará uso a la vpn.

/ppp profile

add local-address=192.168.30.1 name="profile VPN" remote-address=dhcp_pool0 use-compression=yes use-encryption=yes

/ppp secret

add name=admin password="Istr\$2022" profile="profile VPN" service=pptp

Se especifica la zona horaria donde se encuentra el Rio_Firewall_01, la cual se encuentra posicionada en América del Sur, Guayaquil (La misma zona horaria que Riobamba).

/system clock

set time-zone-name=America/Guayaquil. En este apartado final simplemente se asigna un nombre al equipo, y finalmente se configura el ntp client con la dirección del servidor NTP 172.24.10.3, para tener la hora y fecha sincronizada correctamente.

/system identity

set name=RIO_FIREWALL_01

/system ntp client

set enabled=yes primary-ntp=172.24.10.3

5.1.4 Reglas del Firewall

Tabla 12-5: Reglas del Firewall_01

RIO_FIREWALL_01
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input comment="REGLAS DE ESCANEO DE PUERTOS" protocol=tcp psd=21,3s,3,1
Mediante esta regla se hace referencia a que se procesará paquetes que ingresan al enrutador a través de una de sus interfaces, así como también se especifica que se procesará la conexiones que se dan mediante TCP. En donde una vez detectada un escaneo TCP mediante PSD, con parámetros de 21 para WeightThreshold (peso), 3 segundos para DelayThreshold (retardo), 3 para Lop Port Weight (repeticiones) y 1 para High Port Weight (peso alto), permitirá que la dirección de origen de donde proviene el escaneo se agregue al address-list="port scanners" la cual se encontrará almacenada durante 14 días (address-list-timeout=2w).
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg

En esta regla se hace referencia a que se procesará paquetes que ingresan al enrutador a través de una de sus interfaces, así como también se especifica que se procesará la conexiones que se dan mediante TCP, en la cual para fortalecer la detección de escaners de la red se analizará las banderas de la cabecera tcp (**tcp-flags**) la cual se basa en analizar la coincidencia de las banderas tcp una vez que se inicie el escaneo por parte de un atacante por lo cual en esta regla se especifica las siguientes banderas:

- syn: Se utiliza para una nueva conexión.
- rts: Desconectar la conexión o reiniciar una conexión debido a paquetes corrompidos.
- psh: fSe utiliza para forzar el enviado inmediato.
- ack: Se utiliza para el reconocimiento de datos u confirmaciones.
- urg: Se utiliza para definir un bloque de datos como urgentes.
- fin: Sirve para finalización de conexión.

La cual permitirá que la dirección IP de los paquetes que coincidan con los tcp-flags se agregue al **address-list="port scanners"** la cual se encontrará almacenada durante 14 días (**address-list-timeout=2w).**

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=fin,syn

La presente regla se define de igual manera a la anterior, con la única variación definida que los tcp-flags (fin, syn) detecten que toda conexión que no tenga éxito con el servidor se agregue a la lista “port scanners”.

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=syn,rst

La presente regla se define de igual manera a la anterior, con la única variación definida que los tcp-flags (fin, rst) detecten que todo intento de conexión y reconexión constante al servidor se agregue a la lista “port scanners”.

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack

La presente regla de firewall define que busque la adyacencia o coincidencia de banderas tcp de fin, psh y urg, y mientras que las de syn, rst y ack sean omitidas o tomadas en cuenta, una vez que el atacante intente escanear el servidor.

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg

La presente regla de firewall define que busque la adyacencia o coincidencia de los paquetes con la cabecera de banderas tcp de fin, syn, rst, psh, ack, y urg. sean omitidas o tomadas en cuenta, una vez que el atacante intente escanear el servidor.

add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg
La presente regla de firewall define que se agregue al addres-list= “por scanners” todos los paquetes que ingresen al router, definidas con las siguientes banderas: fin, syn, psh, ack y urg.
add action=drop chain=input protocol=tcp psd=1,3s,3,1
Mediante esta regla permite que todas las ips que se encuentran en la lista “port scanners”, que intenten conectarse mediante tcp, dropee todos los paquetes entrantes, de igual manera esta se realizará previo al análisis mediante psd, para la detección de escaneo de puertos.
add action=accept chain=input comment="PERMITIR WEB MIKROTIK" dst-port=8300 protocol=tcp
En esta regla se acepta todos los paquetes que tengan como destino el puerto 8300 mediante tcp.
add action=accept chain=input comment="PERMITIR ICMP NORMAL" icmp-options= protocol=icmp
Esta regla me permite admitir todos los paquetes de icmp, que tengan un comportamiento normal, y una vez realizada un ping al servidor esta me responda con un “echo reply”.
add action=accept chain=input icmp-options=3:0 protocol=icmp
Mediante esta regla me permite admitir con el protocolo icmp los paquetes que definan que el destino es inalcanzable.
add action=accept chain=input icmp-options=3:1 protocol=icmp
Mediante esta regla me permite admitir con el protocolo icmp los paquetes que definan que el host es inalcanzable.
add action=accept chain=input icmp-options=3:4 protocol=icmp
Mediante esta regla me permite definir que la red es inalcanzable fragmentación requerida.
add action=accept chain=input icmp-options=8:0 protocol=icmp
Mediante esta regla me permite admitir los paquetes que solicitan permitir solicitud de eco.
add action=accept chain=input icmp-options=11:0 protocol=icmp
Mediante esta regla me permite admitir los paquetes que se han excedido en el tiempo.

add action=accept chain=input icmp-options=12:0 protocol=icmp
Mediante esta regla me permite admitir los paquetes que incluyan un parámetro incorrecto.
add action=drop chain=input protocol=icmp
Esta regla me permite denegar todos los demás paquetes que no pertenezcan a este tipo.
add action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w chain=input connection-limit=100,32 connection-nat-state=dstnat dst-address=179.49.13.14 ** **dst-port=80 protocol=tcp
En la presenta regla se da a conocer el límite de conexiones TCP que permite el firewall procesar hacia el puerto 80 definido en un máximo de 100.**2w:** intervalo de tiempo después del cual la dirección se eliminará de la lista de direcciones "port scanners", especificando en el límite de conexión, en nuestro caso 2 semanas.
add action=drop chain=input connection-limit=10,32 connection-nat-state=dstnat dst-address=179.49.13.14 dst-port=80 protocol=tcp src-address-list="port scanners"
En esta regla se define que todos los paquetes entrantes y que tengan como destino el servidor web (179.49.13.14), que no cumplan con un límite de tiempo de conexión, se dropee. Y una vez identificada la dirección de origen, esta se agregue a la lista de "port scanners", en la cual permanecerá por un tiempo de 2 semanas.
add action=accept chain=input comment="PERMITIR SNMP" port=161,162 protocol=udp src-address-list=snmp
La presente regla admite todos los paquetes UDP, que buscan conectividades de administración de red (SNMP), la cual se dará mediante los puertos 161 y 162.
add action=accept chain=input comment="PERMITIR IPs GESTION" src-address-list=gestion
En esta regla se define principalmente, que se acepte todos los paquetes que se provengan de la lista de direcciones especificadas como "gestión", la cual permita realizar cualquier acción sobre el equipo.
add action=drop chain=input comment="DENEGAR TODO LO DEMAS" psd=5,3s,3,1
Finalmente se ha designado la presente regla para realizar que, cualquier paquete que no cumpla con ninguna de las reglas antecedentes sean dropeadas u omitidas.

Fuente: (Pinango, 2021)
Realizado por: Marco Estrada

5.1.5 Revisión de procedimientos complementarios.

Para que el sistema funcione correctamente en la institución se deberán realizar varias etapas como:

- Escanear nuevas vulnerabilidades en la plataforma académica institucional
- Elaborar procedimientos para monitorear la seguridad contra phishing en todo el personal que está directamente utilizando el sistema académico.
- Establecer manuales de mantenimiento para mejorar la seguridad de la red contra ataques de externos.

CONCLUSIONES

- Una vez implementado y realizadas las evaluaciones se ha comprobado las amenazas, vulnerabilidades y debilidades que los ciberataques pueden utilizar para penetrar al sistema con la ayuda de la norma ISO: 27001 de la seguridad de la información y la guía OWASP Top10 de vulnerabilidades más críticas conocemos 7 vulnerabilidades del sistema académico del Instituto Superior Tecnológico Riobamba que están conectados directamente a la red pública.
- Se elaboró tres escenarios de prueba, dos con posibles ataques dentro de la red y uno con la implementación del sistema de seguridad firewall reduciendo de 7 vulnerabilidades a 2, comprobando la seguridad del actual del sistema implementado para procesos académicos del Instituto Superior Tecnológico Riobamba.
- Con el diseño del sistema de seguridad anti-phishing se convierte en una fortaleza contra los ataques cibernéticos donde el firewall se encarga de filtrar el tráfico de red entrante y saliente por medio de una serie de reglas la cuales permitían su paso o rechazo de paquetes hacia el sistema.
- Se ha realizado la implementación de un firewall (RIO_FIREWALL_01) y una red local denominada zona desmilitarizada (DMZ) para disminuir los riesgos de ataques informáticos al servidor web del ISTR, en donde el firewall se encargó de filtrar el tráfico de red. También se implementó una LAN DMZ dentro de la red interna de la organización, en donde se ubicó exclusivamente todos los recursos que tienen acceso a internet como es el caso de nuestro servidor web, permitiendo las conexiones procedentes tanto de internet como de la red local de la institución y negando las conexiones que van desde la DMZ a la red local, logrando con esto proteger las conexiones de red y actuando como un filtro entre el servidor web con conexión a internet y la red de ordenadores particulares. En relación con el sistema anterior, la seguridad actual tiene una mejor del 95%.

RECOMENDACIONES

- Se recomienda adquirir espacio en la nube informática para respaldar la base de datos, la aplicación web entre otros sistemas que posee el ISTR.
- Solicitar autorización a las autoridades del Instituto Superior Tecnológico Riobamba para realizar las pruebas correspondientes y no interrumpir con el funcionamiento de las plataformas institucionales.
- Adquirir un certificado de seguridad de internet para evitar que intrusos de la red traten de robar información utilizando técnicas de phishing.
- Realizar un mantenimiento al firewall como también generar reportes periódicos para tener históricos de las amenazas y soluciones.
- Utilizar siempre software licenciado, para evitar multas y que los virus informáticos contagien a tus equipos finales (cell, Tablet, pc)

BIBLIOGRAFÍA

Analuisa, H. (2009). *Implementación de un Firewall en los equipos Informaticos del Laboratorio de Instrumentación virtual ITSA*. Recuperado el 15 de Diciembre de 2021, de http://repositorio.espe.edu.ec/bitstream/21000/7863/1/T-ESPE-ITSA-000106.pdf

AVAST. (2022). Recuperado el 10 de Diciembre de 2021, de https://www.avast.com/es-es/c-phishing

AVAST SOFTWARE. (2022). Recuperado el 10 de Diciembre de 2022, de https://www.avast.com/es-ww/avast-online-security#pc

Ballesteros, A. (2018). *Empresarial y Laboral*. Recuperado el 1 de Diciembre de 2021, de https://revistaempresarial.com/tecnologia/seguridad-informatica/vulnerabilidades-ciberneticas-y-su-impacto-organizacional/

Bonilla, J. (2016). *Pontificia Universidad Católica del Ecuador*. Recuperado el 2021, de Diseño e Implementación de un Firewall L2 utilizando redes definidas por Software(SDN): http://repositorio.puce.edu.ec/bitstream/handle/22000/13153/INFORME%20CASO%20DE%20ESTUDIO%20-%20ADRIAN%20BONILLA.pdf?sequence=1&isAllowed=y

CIBERSEGURIDAD. (2020). *Noticias de ciberseguridad*. Recuperado el 15 de Diciembre de 2021, de https://ciberseguridad.com/herramientas/software/nikto/

Corozo, M. (2016). Recuperado el 15 de Diciembre de 2020, de http://dspace.espoch.edu.ec/bitstream/123456789/5468/1/98T00106.pdf

CTMA consultores. (13 de Octubre de 2021). *Objetivo de la norma ISO*. Recuperado el 10 de Agosto de 2021, de https://ctmaconsultores.com/objetivo-de-la-norma-iso-27001/

Departamento de Tecnología Organización Inca. (2018). *Políticas de Seguridad Informática (PSI)*. Recuperado el 10 de Diciembre de 2021, de https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf

Espinoza, E. (2 de Septiembre de 2019). *Scielo*. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442019000400171

Fernández, C. (2010). *Introducción a OWASP*. (The OWASP Foundation) Recuperado el 10 de Diciembre de 2021, de https://owasp.org/www-pdf-archive/Introduccion_a_la_OWASP.pdf

Gómes, R. (2018). *Seguridad Informática*. Recuperado el 10 de diciembre de 2021, de http://www.cryptomex.org/SlidesSeguridad/nmap.pdf

Gómez, V. (2019). *DOJOCONF*. Recuperado el 21 de 10 de 2021, de https://dojoconfpa.org/nmap-network-mapper/

Ibáñez y Almenara. (2016). *Técnicas para combatir el phishing*. Recuperado el 10 de Diciembre de 2021, de https://ialmenara.com/danos-causados-por-el-phishing-y-como-combatirlo/

Jiménez, E. (Febrero de 2014). *Instituto Politécnica Nacional*. Recuperado el 10 de Diciembre de 2021, de https://tesis.ipn.mx/jspui/bitstream/123456789/15606/1/I.C.E.%2044-14.pdf

Malwarebytes. (2021). *Phisihing*. Recuperado el 12 de Diciembre de 2021, de https://es.malwarebytes.com/phishing/

Medina, J. (2016). Recuperado el 12 de Diciembre de 2021, de https://repository.udistrital.edu.co/handle/11349/7440

Muñoz, F. (2021). *We live security by eset*. Recuperado el 20 de Diciembre de 2021, de https://www.welivesecurity.com/la-es/2021/05/14/que-es-virus-troyano-informatica/

OCU. (2022). *Phising*. Recuperado el 10 de Diciembre de 2022, de https://www.ocu.org/tecnologia/internet-telefonia/consejos/evitar-ataque-phishing

OWASP. (2017). *OWASP Top 10-2017*. Recuperado el 10 de Diciembre de 2021, de https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Pilamunga, N. (2019). *Dspace*. Recuperado el 1 de Diciembre de 2021, de http://dspace.espoch.edu.ec/bitstream/123456789/9694/1/20T01145.pdf

Pinango, Á. (2021). *Dspace- ESPOCH*. Recuperado el 10 de Octubre de 2021, de http://dspace.espoch.edu.ec/handle/123456789/14516

RAE. (2020). *Real Academia de la Lengua*. Recuperado el 1 de Diciembre de 2021, de https://dle.rae.es/amenaza

Torres, G. (2021). *AVG*. Recuperado el 12 de Diciembre de 2021, de Virus Informático: https://www.avg.com/es/signal/what-is-a-computer-virus

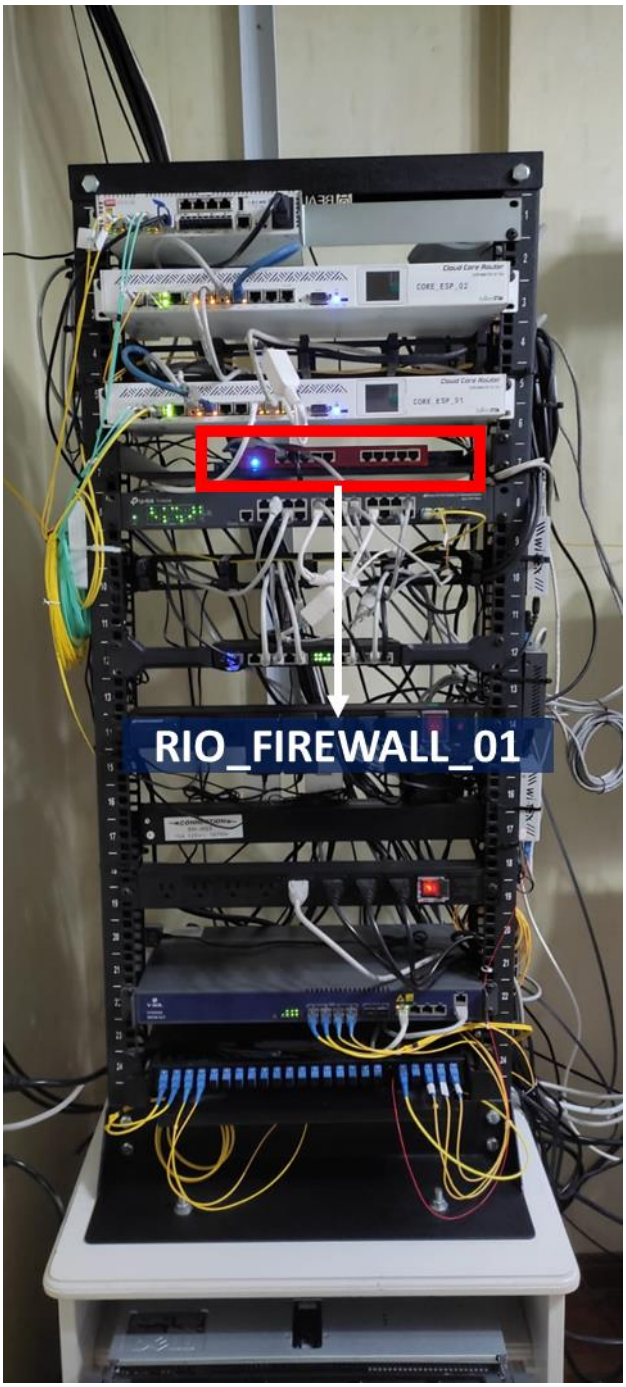
UNIR. (2020). Recuperado el 1 de Diciembre de 2021, de https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

UNIR. (2020). *La Universidad en Internet*. Recuperado el 1 de Diciembre de 2021, de https://www.unir.net/ingenieria/revista/hacking-etico/

Valente, R. (2018). *DSPACE*. Recuperado el 15 de Diciembre de 2021, de http://dspace.espoch.edu.ec/handle/123456789/9056

ANEXOS

ANEXO A: Ubicación del Rio_Firewall_01 en el Rack de la organización.



ANEXO B: Router Firewall adquirido

ANEXO C: Router BOARD adquirido

ANEXO D: Certificado de Auspicio

Riobamba, 12 de Agosto de 2021

Ingeniero
Luis Hidalgo Almeida PHD
DIRECTOR DEL INSTITUTO DE POSGRADO Y EDUCACION CONTINUA – IPEC
Presente

De mi consideración:

Reciba un atento y cordial saludo de parte de quienes conformamos Instituto Superior Tecnológico Riobamba, al mismo tiempo desearle éxitos en las funciones a usted encomendadas.

Por medio de la presente deseamos manifestar nuestro apoyo y auspicio al tema de tesis.

"Implementación y evaluación de un sistema de seguridad anti phishing para protección de la información utilizando un Firewall en procedimientos académicos en línea para el Instituto Superior Tecnológico Riobamba" a desarrollarse por el Sr. Marco Vinicio Estrada Velasco con C.I 060357067-2 para nuestro Instituto Tecnológico Superior Riobamba, el mismo que ratificamos y apoyamos en su totalidad.

Firmado electrónicamente por:
TANIA LEONOR
PARRA PROAÑO

Ing. Tania Parra Proaño MsC.
Rectora del Instituto
Superior Tecnológico Riobamba

Presente