FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

"Desarrollo de una Red Honeypot para la Detección de Intrusiones en la Municipalidad Distrital de Víctor Larco Herrera - Trujillo"

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Br. VALDIVIEZO AVALO, Jormy Jean Franco (ORCID: 0000-0002-5061-6087)

ASESOR:

Mg. Edwin Mendoza Torres (ORCID: 0000-0003-4334-6813)

LÍNEA DE INVESTIGACIÓN

Infraestructura y Servicios de Redes y Comunicaciones

Trujillo – Perú

2020

Dedicatoria

A **Dios** por permitirme seguir en la lucha para seguir adelante.

A mis **Padres** por el gran esfuerzo que han realizado en el cumplimiento de esta meta propuesta y el enorme apoyo brindado día a día, a su afecto, compresión y aliento que me ofrecieron durante mi desarrollo como estudiante.

A los **Docentes** por el tiempo y conocimientos brindados a lo largo de este tiempo y amigos de la Universidad por el apoyo constante en el desarrollo de mis metas.

Valdiviezo Avalo, Jormy Jean Franco

Agradecimiento

Un especial agradecimiento a esta
Universidad por ser mi segunda casa y
haberme brindado todas las facilidades
en la realización de este proyecto.
A mi Docente Metodólogo por habernos dado
la motivación para seguir adelante y todos sus
valiosos consejos durante este último año.
A mi Asesor especialista por haberme guiado
en la culminación de este desafío por la paciencia
y solución de todas las dudas presentadas.

Valdiviezo Avalo, Jormy Jean Franco

Página del Jurado

Declaratoria de Autenticidad

DECLARATORIA DE AUTENTICIDAD

Yo, **Valdiviezo Avalo Jormy Jean Franco,** estudiante del X ciclo de la Facultad de Ingeniería de la Escuela de Ingeniería de Sistemas de la Universidad Cesar Vallejo identificado con DNI N° **70411699**, con la tesis titulada **"Desarrollo de una Red Honeypot para la detección de intrusiones en la Municipalidad de Víctor Larco Herrera"**

1.- La tesis presentada es de mi autoría.
2.- He cumplido con lo establecido por las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto, la tesis no ha sido plagiada ni total ni parcialmente.
3.- Los datos obtenidos en los resultados son reales, no han sido alterados bajo ninguna forma, por lo tanto, los resultados que se presentan en la tesis constituyen aportes a la realidad investigada.

De identificarse fraude (datos falsos), plagio (información sin citar a autores), piratería (uso ilegal de información ajena) o falsificación (representar falsamente las ideas de otros), asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad César Vallejo.

Trujillo, 20 de enero de 2020.

Br. Valdiviezo Avalo, Jormy Jean Franco
70411699

ÍNDICE

Índice de Imágenes

Índice de Tablas:

Índice Anexos

RESUMEN

El presente trabajo fue titulado “Desarrollo de una Red Honeypot para la detección de intrusiones en la Municipalidad Distrital de Víctor Larco Herrera - Trujillo 2018”. Semanas atrás un ataque masivo tuvo como objetivo las instituciones financieras, el cual fue repelido gracias a varias herramientas y técnicas empleadas para garantizar la seguridad d ellos bancos, una de estas, es un sistema señuelo, que tiene como objetivo, detectar intrusiones a la red de datos y analizarlas para identificar el método usado por el/los atacantes(s), y cuál es el objetivo de es€(os), con esta información se mejorara la seguridad en el sistema real un sistema trampa que tiene como objetivo detectar intrusiones y analizarlas para identificar el método usado por el atacante y cuál es el objetivo de este, con esta información se mejorara la seguridad en el sistema real; se hace un recuento de los casos más sonados sobre los diferentes ataques cibernéticos y que tan apreciado es mantener una Infraestructura de Red Segura; también vemos las teorías relacionadas con Honeypots y seguridad de la información, pasamos a identificar el método de investigación la cual es de tipo preexperimental, la muestra es igual a la población fue uso de estudio y que es la dirección IP publica de la red, para determinar las vulnerabilidades que presentaba, se aplicó la metodología de hacking Ético y la aplicación de varias herramientas adicionales que nos proporcionaron información entre ellas, Nmap que es un scanner de puertos, también OpenVas para identificar que vulnerabilidades se presentaban y Snort un sistema de detección de intrusiones; como conclusión se logró mejorar la detección de intrusiones.

Palabras clave: Ciberseguridad, Red Honeypot, Detección de Intrusiones, hacking ético

ABSTRACT

This research was entitled “Honeypot Network Development for detecting intrusions in the district Municipality of Victor Larco Herrera – Trujillo, 2018”. Its main objective was to develop a Honeypot Network to detect intrusions in the data network of the Municipality of Victor Larco Herrera and prevent attacks similar to the Black Hat Community’s, which hacks worldwide breaking into secure networks to destroys several organizations, especially the financial ones. This research develops actions to repel network attacks by creating a network, which acts as a baiting system, and has the objective to detect intrusions in the data network, analyses them to identify the method used by the attackers, and what their objective is. The security in the network infrastructure will get better with the information obtained. The research method is pre-experimental; and the public IP address of the network was set as the population. To determine the possible vulnerabilities, the Ethical Hacking Methodology and the application of several additional tools were applied, such as Nmap, which is a port scanner, Open Vas, to identify the vulnerabilities and Snort, and a System to detect intrusions (IDS). In conclusion, the intrusion detection in the District Municipality Larco Herrera – Trujillo, 2019 improved.

Key words: Cybersecurity, Honeypot Network, Intrusion detection, Ethical Hacking.

I. INTRODUCCIÓN

El Internet Crime Complaint Center (IC3) del FBI[1] en el año 2015 reporto pérdidas estimadas en 1.070 millones de dólares solo en los Estados unidos y de unos 400.000 millones de dólares en todo el mundo[2] y para el 2019 según Forbes se alcanzarán 2.1 trillones de dólares en pérdidas.

JPMorgan Chase una de las empresas financieras más antiguas del mundo, sufrió en el 2014 un ciberataque que puso en peligro 83 millones de cuentas, tenemos la "Operación Aurora" efectuada por un grupo asociado al Ejército Popular de Liberación, donde empresas como Google, Adobe y Northop Grumman (conglomerado de empresas aeroespaciales y de defensa) sufrieron ataque con la intención, según McAfee, de acceder y modificar el código fuente de sus repositorios. El ataque de Stuxnet a las instalaciones nucleares de Irán, el apagón causado a más de 80.000 ciudadanos por parte de un programa malicioso que afecto a los centros de control de plantas de energía de Ucrania, esto ha originado la creación de "Cibercomandos" por varios países para fines defensivos como ofensivos (Bakinter, 2015); a esto se le suma la creación de Equipos de Respuesta ante Emergencias Informáticas CSIRT (Observatorio de la Ciberseguridad en América Latina, 2016)

El Departamento de Seguridad Nacional de los Estados Unidos (Department of Homeland Security – DHS)[3], es el encargado de prevenir y responder a emergencias nacionales. En la Directiva de Política Presidencial / PPD-21; Seguridad y Resiliencia de la infraestructura Critica, identifica 16 sectores de "cuyos activos, sistemas y redes, tanto físicos como virtuales, se consideran tan trascendentes que su inhabilitación o pérdida tendría un resultado debilitante sobre la seguridad nacional" (DHS, 2013) Tomando como referencia el informe, uno de los sectores, es el de Tecnología de la Información y el de Instalaciones Gubernamentales, esto denota la gran importancia que tienen estos dos sectores y lo imperativo que es de la aplicación de políticas que aseguren una contención de todos los riesgos y de su continuidad de servicios.

[1] Internet Crime Complaint Center [En línea] [Citado el: 02 de 10 de 2017.] https://www.ic3.gov/default.aspx
[2] Fuente: Khoo Boon Hui (Ex presidente de INTERPOL). "Los cibercriminales se lucran en Internet". Fundación Innovación Bankinter – Fundación Future Trends Forum.
[3] Department of Homeland Security, [En línea] [Citado el: 02 de 10 de 2017.] https://www.dhs.gov/

Mediante el uso de herramientas y técnicas que permitan un mejor enfoque a las amenazas que se presentan, es por ello de un análisis de los diferentes métodos que son usado por los atacantes, ya sea su origen como el fin de estos.

Existe una gran variedad de ataques pero se ha visto una tendencia muy preocupante con el secuestro de información mediante el uso de Ransonware como el WannaCry, los ataques de Denegación de Servicio Distribuido DDoS sufridos por Dyn el 21 de octubre, o la poca seguridad que presentan los dispositivos IoT que los hace muy vulnerables y objeto de los atacantes, como en el que millones de estos dispositivos fueron infectados para el ataque perpetrado a los servidores de Dyn. (Cameron Camp y Stephen Cobb, 2017)

CVEs recibidos y procesados

	Nuevas CVE recibidas por NVD	Nuevas CVEs analizadas por NVD	CVEs modificadas recibidas por NVD	CVEs modificados Re-analizados por NVD
Hoy	0	0	0	0
Esta semana	160	250	5292	1
Este mes	0	0	0	0
El mes pasado	1158	1213	13120	23
Este año	11019	10859	58729	652

Fuente: CVE (Common Vulnerabilities and Exposures)[4]

En América Latina las pérdidas originadas por cibercrimen ascenderán a los 76 mil 766 millones de dólares en el 2017 y en Perú se alcanzarían los 4 mil 782 millones de dólares ubicándose en el puesto siete de toda la región, habiendo invertido el año pasado 22 millones de dólares en ciberseguridad. Los servicios más usados en ciberseguridad fueron los de gestión de activos y monitoreo (71%), inteligencia, investigación, detección y remediación de amenaza (18%), gestión de riesgos y cumplimiento (8%) (Empresarial, 2017)

Cabe destacar que el sector Gobierno se sitúa como el más propenso ante posibles ataques cibernéticos, con el 49.53%; el sector financiero con 14.34%; el de telecomunicaciones 12.83%; el sector industrial, con un 10.70%; y energía, con el 6.54% (Barbieri, 2015).

[4] Base Nacional de Vulnerabilidades, CVE al 01 de octubre del 2017: National Institute of Standards and Technology (NIST) [En línea] [Citado el: 01 de 10 de 2017.] https://nvd.nist.gov/general/nvd-dashboard

En Perú más del 40% de la población (12 Mills) tiene conexión a internet hasta el 2015, lo que conlleva a estar expuestos a riesgos en la seguridad cibernética[5], los datos presentados en el informe denominado "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?", indican que en 2013 hubo un aumento del 30% de incidentes cibernéticos, así como el incremento de malware en el 2014 cuando se realizaba la Copa Mundial de Futbol, siendo el PeCERT[6] el encargado de dar respuesta a estos incidentes.

A todo lo mencionado, es imprescindible para el Área de Tecnologías de Información hacer uso de tecnologías que proporcionen un nivel de seguridad más robusto y que genere reportes y alertas de intrusiones; como fortalecer las vulnerabilidades más críticas que hayan sido encontradas.

Tabla 1: Problemática Actual

PROBLEMA	CAUSA	CONSECUENCIA
Falta de información sobre el diseño de la infraestructura de red con la que actualmente está operando la Municipalidad	• No se ha realizado un análisis de la red actual • No se lleva un registro de los análisis realizados sobre la infraestructura de red	• No se tiene información actualizada
Existencia de vulnerabilidades en la infraestructura de red de la Municipalidad	• No se han realizado pruebas de hacking ético o pentesting • No se ha revisado el nivel de seguridad de la infraestructura de red	• Vulnerabilidades que pueden ser explotadas por un atacante.
Falta de información sobre intrusiones o herramientas que puedan detectarlas	• No existe un Sistema de detección de intrusiones (IDS) • No se registran los Logs sobre intrusiones	• Capacidad de respuesta muy limitada ante algún ataque e intrusión

Elaboración: Microsoft Office Word 2016.

[5] Grupo del Banco Mundial, "Internet users (per-100 people)," World DataBank (2015), [En línea] [Citado el: 16 de 09 de 2017.], https://data.worldbank.org/indicator/IT.NET.USER.P2.

[6] Coordinación de Emergencias en Redes Teleinformáticas, [En línea] [Citado el: 16 de 09 de 2017], http://www.pecert.gob.pe/index.html

El presente trabajo propuso el desarrollo de una red Honeypot para la detección de intrusiones en la Municipalidad de Víctor Larco Herrera.

Como antecedente, en el ámbito ***Internacional***, tenemos la investigación de Torres Quezada, Rebeca Soledad, en la ciudad de Ecuador, denominada "Implementar una Red Honeypots para la Detección y Categorización de Intrusos mediante Máquinas Virtuales en el Ministerio de Defensa Nacional" (Quezada Torrez, 2014).

El presente proyecto de investigación hace un análisis de la implementación de Honeypots, que permiten realizar un análisis de los datos recolectados que ya hayan sido capturados, esto permite determinar las formas y tipos de ataques que se produzcan, así como datos del atacante.

Del cual se empleará la medición del tráfico de la red, el funcionamiento y modo de operación de la Red Honeypot, la ubicación de este dentro de la red, su instalación y configuración.

Otro de los antecedentes del cual hemos basado el desarrollo de este proyecto es el de Theodore Henry Wilson I que realizo el siguiente trabajo de investigación en la ciudad Maryland, denominado "Restrictive deterrence and the severity of hackers' attacks on compromised computer systems". (Theodore, 2014).

Esta investigación se enfoca sobre cómo afecta la disuasión sobre los atacantes, el anuncio de que existe vigilancia en un sistema, se examina si se produce un efecto disuasivo restrictivo en los sistemas

El aporte brindado por Theodore Henry es sobre la implementación de una serie de computadoras virtuales con vulnerabilidades conocidas que fueron implantadas aleatoriamente en la universidad, de esto se tomara como referencia la metodología y tecnología usada en dicha investigación.

A nivel ***Nacional,*** me basare en la tesis realizada en la ciudad de Cuzco sobre "Implementación de una Honeynet en la Infraestructura de la red de datos de la E.P.S SEDACUSCO para incrementar la seguridad de sus servidores" (Wernher, y otros, 2016).

Se define el análisis en la que se encuentra la red de datos de la institución con el propósito de implementar Honeypots para la captura del tráfico y sus actividades así lograr un análisis de sus movimientos.

El aporte que nos brinda el presente proyecto es el análisis que hacen sobre la infraestructura de la red y el Hardware, el modo estudio sobre la selección del Honeypot y su posición

dentro de la red, la creación del entorno simulado de la red y las configuraciones realizadas como su implementación.

También tenemos el trabajo de "Infraestructura de defensa" (Russell Pinto, 2014). Realizado en la ciudad de defensa, donde realiza un análisis de las diferentes herramientas para asegurar una defensa perimetral que ayudan a la protección ante atacantes; el análisis que hace sobre las ventajas y desventajas de implementar una red Honeypot, es tomada en cuenta en el desarrollo del presente trabajo y así determinar los posibles inconvenientes que podríamos tener.

En el ámbito ***Local,*** tenemos la "Elaboración de una Red espejo en la zona perimetral para la detección de intrusiones" (Dios Leon, y Ortiz danae, 2014), Donde se presenta una copia de la red central y de un diseño lógico donde se obtiene una Honeynet, con el objetivo de detectar intrusiones y conocer sus modalidades para aplicar medidas que puedan contrarrestar estas vulnerabilidades.

Del aporte que brinda el trabajo previo local, se tomara como referencia la población y muestra, la recolección de datos, las variables, las técnicas y procedimientos de recolección de datos, su análisis y los materiales utilizados.

"*A un panal de rica miel dos mil moscas acudieron que por golosas murieron presas de patas en él"* (Samaniego, 2017).

Usando como analogía este breve relato de fábula, nos hace ver la manera en la que funciona un Honeypot, como un señuelo con información tentadora que está expuesto a los ataques con medidas de seguridad pero que no sean imposibles de vulnerar, haciendo que toda la actividad sea vigilada logrando obtener información del atacante.

Según (Spitzner, 2002 pág. 58) "Un Honeypot es una técnica de seguridad cuyo valor radica en ser sondeado, agredido o comprometido". Esto permite al administrador conocer nuevas vulnerabilidades, así como nuevos tipos de ataque, tener un registro del ataque al sistema, despistar al atacante sobre los servidores hasta atraer atacantes.

(Spitzner, 2002 pág. 62) define dos tipo de Honeypots; de Investigación que estan destinados al estudio, para obtener informacion sobre las amenazas que se identifican y lo de Produccion que se implementancomo valor agregado a la seguridad de una oragnizacion

especifica. En si, no existe una deficinicion en su modo de operación, sino en el proposito que este tiene para su imlementacion.

En el programa e-learning de Cisco Netacad (Academy, 2017) la Ciberseguridad es el constante trabajo de asegurar y brindar el resguardo de los sistemas de red y de información contra el uso no autorizado o de los perjuicios a los que podrían estar expuestos y se puede presentar en tres niveles:

- A nivel Individual; se deben resguardar sus datos personales, así como sus dispositivos informáticos.
- A nivel de una Entidad; es compromiso de todos proteger el prestigio, los datos y los clientes.
- A nivel de Gobierno; la seguridad nacional, la seguridad y el bienestar de los ciudadanos están en juego.

Según (Gupta, 2005) la Seguridad de la Información es el tratamiento que se da para asegurar que los recursos de información cumplan con la protección de su confidencialidad, integridad y disponibilidad.

De acuerdo con (Valencia Duque, F. and Orozco-Alzate, M., 2017) la seguridad Informática se enfoca en las tecnologías e infraestructuras tecnológicas que sirven de gestión de la información, mientras que la Seguridad de la Información se refiere a la información en sí misma, como activo estratégico

En el Reporte consultado de (Report, 2016) la norma ISO/IEC 27000, es un estándar sobre la seguridad de la información, en él se describe la implementación de un Sistema de Gestión de Seguridad de la Información, donde se incluyen todos los controles administrativos, técnicos y operativos para asegurar la información dentro de una organización.

Es importante también mencionar cuales son los tipos de ataques más usados en la actualidad. En la Estrategia Nacional de Ciberseguridad publicada por (government, 2016) define la denegación de servicio, como el resultado de masivas peticiones de información, con el objetivo de saturar el sistema al momento de que este dé respuesta a esta inundación de solicitudes, imposibilitando que los usuarios autorizados logren acceder.

Otra técnica usada por los atacantes es la captura de tráfico que es examinado logrando un análisis de los paquetes, con estos se puede capturar inicios de sesión, contraseñas y hasta logrando modificar parte o todo el tráfico.[7]

También tenemos la falsificación de identidad según este ataque se aprovecha de la confianza de la víctima, en la que atacante logra la suplantación de correos electrónicos o de sitios Webs, haciendo interactuar a las victimas creyendo que están interactuando con la compañía o persona legitima**.** (KnowBe4, Inc)**.** Suele confundirse con ataques de pishing, pero estos usan spoofing como parte de la estrategia de su ataque, el objetivo es que la víctima renuncie a su privacidad por haciéndose pasar por alguien legitimo (Zink, 2009)

Tenemos finalmente los ataques de día cero, que según (Avast) es el descubrimiento de alguna vulnerabilidad del sistema, software, por parte de hackers criminales; y del desconocimiento de esta vulnerabilidad por parte de los desarrolladores, proveedores de antivirus y público en general. Se le denomina así a este ataque porque desde el descubrimiento de la vulnerabilidad, se le considera día cero hasta que se lance un parche que corrija este fallo.

En la Identificación de posibles fallos de seguridad se realiza un análisis de vulnerabilidades, según (Gabriel, 2016) el análisis de Vulnerabilidades tiene la ventaja en su tiempo de ejecución, que es más rápido en comparación con el Pentesting y el Ethical Hacking, es más barato, además de no requerir una metodología para su aplicación.

[7] Netacad. Cybersecurity Essentials [En línea] [Citado el: 20 de 04 de 2018.] https://static-course-assets.s3.amazonaws.com/CyberEss/es/index.html#3.3.1.2

ENUNCIACIÓN DEL PROBLEMA

Tabla 2: Enunciación del Problema.

ENUNCIACIÓN DEL PROBLEMA	ELEMENTOS PRESENTES
¿De qué manera el desarrollo de una red Honeypot influyó en la detección de intrusiones en la Municipalidad Distrital de Víctor Larco Herrera – Trujillo en el año 2018?	➢ Variables: ✓ Independiente: Red Honeypot. ✓ Dependiente: Detección de intrusiones. ➢ U. de Análisis: Municipalidad Distrital de Víctor Larco Herrera. ➢ Lugar: Víctor Larco Herrera. ➢ Periodo: 2018

Fuente: 2.2 Variables, Operacionalización
Elaboración: Microsoft Office Word 2016.

Para justificar el desarrollo del presente trabajo nos basamos en primer lugar en el aspecto ***Económico***, los costos realizados en el Desarrollo de una Red Honeypot son mínimos, puesto que se hizo uso de aplicaciones de código abierto (Open Source).
En segundo lugar, tenemos el aspecto ***Tecnológico,*** ante el incremento de ataques y las diferentes modalidades en la que se presentan, hace indispensable la implementación de técnicas y herramientas que hagan posible la detección de ataques e intrusiones para la pronta ejecución de medidas que den solución a estos problemas cada vez más comunes y complejos que pueden causar daños severos a las empresas como en la continuidad de sus servicios.
Como Tercera Justificación, tenemos el aspecto ***Operacional,*** en la elaboración del presente proyecto, se contó con la infraestructura adecuada para el desarrollo de la Red Honeypot y de las facilidades necesarias. Las Herramientas que fueron usadas estuvieron disponibles en la aplicación del proyecto.
En el desarrollo de la tesis se plantea la siguiente como hipótesis: El desarrollo de una red Honeypot mejoró la detección de intrusiones en la Municipalidad Distrital de Víctor Larco Herrera – Trujillo

Tabla 3: Hipótesis:

Hipótesis	Componentes Metodológicos			Componentes Referenciales	
El desarrollo de una red Honeypot mejoró la detección de intrusiones en la Municipalidad Distrital de Víctor Larco Herrera en el año 2017.	**Variables**	**Unidad de Análisis**	**Conectores Lógicos**	**El espacio**	**El tiempo**
	Red Honeypot. Detección de intrusiones.	Municipalidad Distrital de Víctor Larco Herrera.	Mejora	Víctor Larco Herrera	2018

Fuente: Formulación del Problema
Elaboración: Microsoft Office Word 2016.

Como Objetivo General de la investigación está en Mejorar la detección de intrusiones mediante el desarrollo de una Red Honeypot para la Municipalidad Distrital de Víctor Larco Herrera, por otro lado, como objetivos específicos están en:

- Analizar la Infraestructura de la Red Actual de la Municipalidad Distrital de Víctor Larco Herrera.
- Disminuir el número de vulnerabilidades en la Infraestructura de Red de la Municipalidad Distrital de Víctor Larco Herrera.
- Determinar el número de intrusiones en la Infraestructura de Red de la Municipalidad Distrital de Víctor Larco Herrera.

II. MÉTODO

2.1 Tipo y Diseño de Investigación

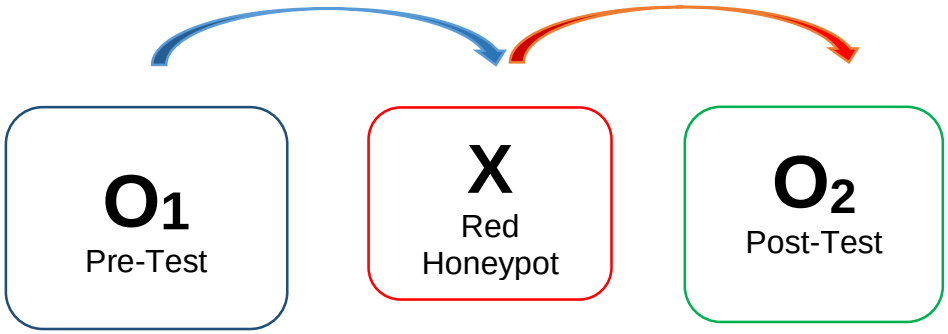
En la realización del desarrollo se aplicará el diseño Experimental de tipo Pre Experimental, mediante la implementación del método de Pre-Test y Post-Test**.**

- ✓ La aplicación Hacking Ético sin el desarrollo de una Red Honeypot para la detección de intrusiones (Pretest).

  En este caso se aplicarán pruebas de Hacking Ético a la infraestructura de Red Actual de la Municipalidad Distrital de Víctor Larco Herrera.
- ✓ La aplicación Hacking Ético con el desarrollo de una Red Honeypot para la detección de intrusiones (Post Test).

  En este caso se aplicarán pruebas de Hacking Ético a la infraestructura de Red Actual de la Municipalidad Distrital de Víctor Larco Herrera utilizando el desarrollo de una Red Honeypot para la detección de intrusiones.

Imagen 1: Diseño de Investigación



Fuente: 2.1 Diseño de Investigación
Elaboración: Microsoft Office Word 2016.

O1= Pre-Test.

X = Red Honeypot

O2 = Post-Test

2.2 Operacionalización de Variables

Identificación de Variables

Variable Independiente Red Honeypot

Variable Dependiente: Detección de intrusiones.

Objeto de Estudio: Municipalidad Distrital de Víctor Larco herrera

Operacionalización de Variables

Tabla 4: Operacionalización de Variables

Variables	Definición Conceptual	Definición Operacional	Indicadores	Escala de Medición
Variable Dependiente: Detección de intrusiones	Es el proceso de identificación de intrusiones a la red, en el cual se establecen los procedimientos donde se analiza la actividad de entradas no autorizadas y/o maliciosas (MIT, 2005)	Cuando se detecte tráfico en la red Honeypot se calificará como sospechoso y se dará alerta al administrador	Análisis de la Red Actual Numero de Vulnerabilidades Identificadas Numero de intrusiones identificadas	De Razón
Variable Independiente: Red Honeypot.	"Una Honeypot es una técnica de seguridad cuyo valor radica en ser sondeado, agredido o comprometido" (Spitzner, 2002 pág. 58)	Es la implementación de un sistema donde se vigilará todo el tráfico que pase ya que es sospechoso en potencia por tal motivo tiene que estar separado del resto de la red	Pruebas de Conectividad	De Razón

Fuente: 2.2 Variables, Operacionalización
Elaboración: Microsoft Office Word 2016.

Tabla 5: Indicadores

N°	INDICADOR	DESCRIPCIÓN	OBJETIVO	TÉCNICA / INSTRUMENTO	TIEMPO EMPLEADO	MODO DE CÁLCULO
1	Análisis de la Red Actual **(ARA)**	Analiza la Infraestructura de la Red Actual de la Municipalidad Distrital de Víctor Larco Herrera	Analizar la Infraestructura de la Red Actual de la Municipalidad Distrital de Víctor Larco Herrera	Mediante la Observación y Recopilación Documental	2 semanas	Sera presentado de manera gráfica antes y después del desarrollo de la Red Honeypot
3	Numero de Vulnerabilidades Identificadas **(NVI)**	Determinar el número de vulnerabilidades identificadas	Disminuir el número de vulnerabilidades	Hacking Ético	2 semanas	$\boldsymbol{NVI = n}$ **NVI**: Numero de Vulnerabilidades Identificadas **n:** Numero Vulnerabilidades Identificadas
4	Numero de Intrusiones Identificadas **(NII)**	Identificar el número de intrusiones	Determinar el número de intrusiones	IDS / Snort	2 semanas	$\boldsymbol{NII = n}$ **NII**: Numero de Intrusiones Identificadas **n:** Numero de Intrusiones Identificadas.

Fuente: 2.2.2 Variables de Operacionalización
Elaboración: Microsoft Office Word 2016.

2.3 POBLACIÓN Y MUESTRA

Población

La población será de una sola, dado que se trabajará con la IP pública de la Municipalidad Distrital de Víctor Larco.

Muestra

Se tomará la única población que es la dirección IP pública, por lo consiguiente no será necesario obtener la muestra por alguna fórmula.

2.4 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS, VALIDEZ Y CONFIABILIDAD

Técnicas e instrumentos de Validación de Datos

Tabla 6: Técnicas e Instrumentos de Datos

TÉCNICA	INSTRUMENTO	FUENTE	INFORMANTE
REGISTRO DE INFORMACIÓN	Analizador de Puertos / Nmap	Accesos indebidos de la infraestructura de Red de la Municipalidad Distrital de Víctor Larco Herrera	Reporte de Nmap

Fuente: 2.2 Variables de Operacionalización
Elaboración: Microsoft Office Word 2016

Validez del Instrumento

Juicio de Experto

Son el conjunto de opiniones brindadas por profesionales expertos del tema.

Confiabilidad del Instrumento

Opinión del Experto

Se tomaron en cuenta las opiniones expresadas por expertos en el tema para la validación de los instrumentos utilizados en la recolección de datos que han sido tomados para el presente proyecto,

2.5 MÉTODOS DE ANÁLISIS DE DATOS

Para verificar la hipótesis y definir si esta es admitida o rechazada, se analiza el Pretest y el PosTest de las variables luego de que estas hayan sido expuestas al objeto de estudio; para ello se efectuará **estadística descriptiva.**

En la presente investigación los datos no poseen suficiente información para determinar si presentan o no presentan normalidad por lo que esta prueba será omitida ante lo especial de los datos obtenidos.

III. RESULTADOS

3.1 Contrastación de Hipótesis

Prueba de Hipótesis.

La contrastación de la Hipótesis se ha realizado de acuerdo al Método propuesto Pre Test – Post Test, para poder aceptar o rechazar la hipótesis.

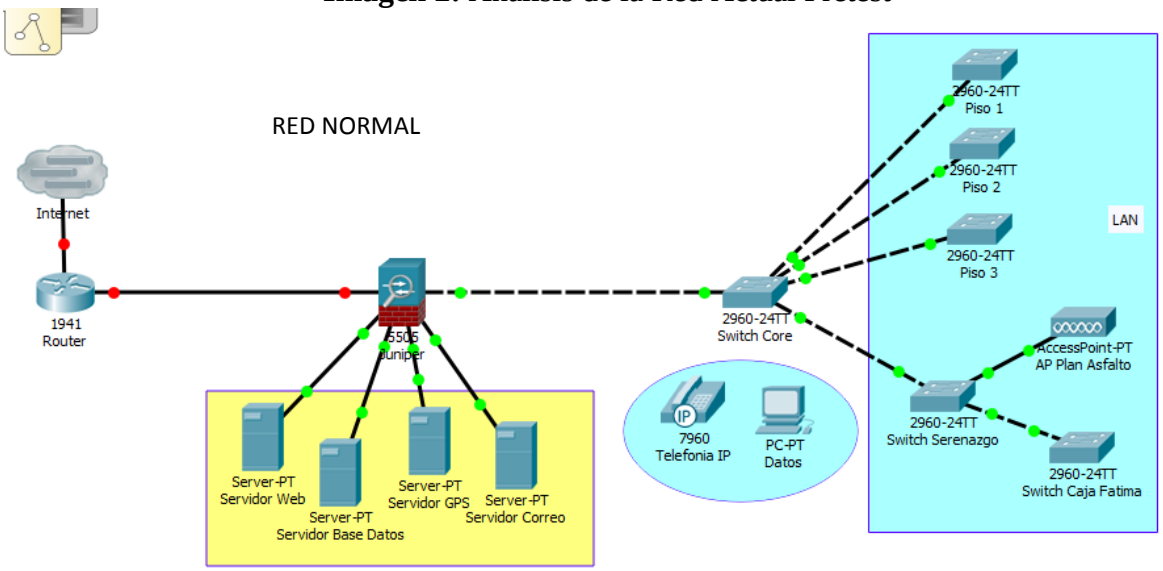
3.1.1. Prueba de hipótesis para el indicador N° 01.

Análisis de la Red Actual

Definición de Variables

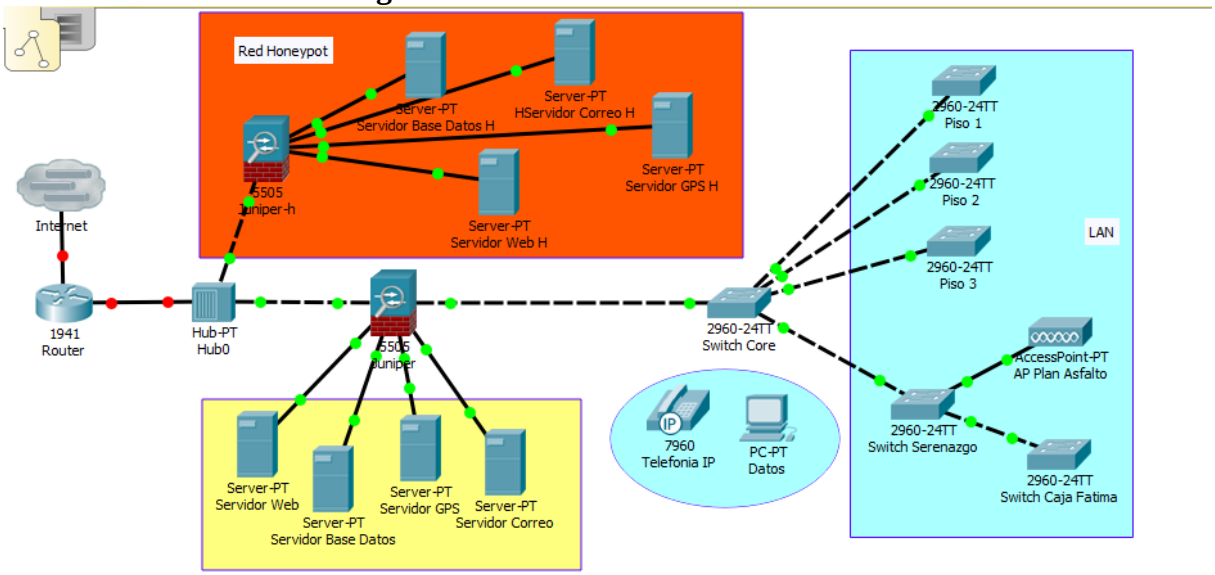
ARAa = Análisis de la Red Actual sin el desarrollo de la Red Honeypot.

Imagen 2: Análisis de la Red Actual Pretest



Fuente: 3.2.1 Análisis de la Infraestructura de la Red de la Municipalidad
Elaboración: Cisco Packet Tracert.
ARAp = Análisis de la Red Actual con el desarrollo de la red Honeypot

Imagen 3: Análisis de la Red Actual Postest



Fuente: 3.2.1 Análisis de la Infraestructura de la Red de la Municipalidad
Elaboración: Cisco Packet Tracert.

3.1.2. Prueba de hipótesis para el indicador N° 02.

Numero de vulnerabilidades Identificadas

A. Definición de Variables:

NVIa: Numero de Vulnerabilidades Identificadas sin la Red Honeypot.

NVIp: Numero de Vulnerabilidades Identificadas con la Red Honeypot.

B. Resultados de la Hipótesis

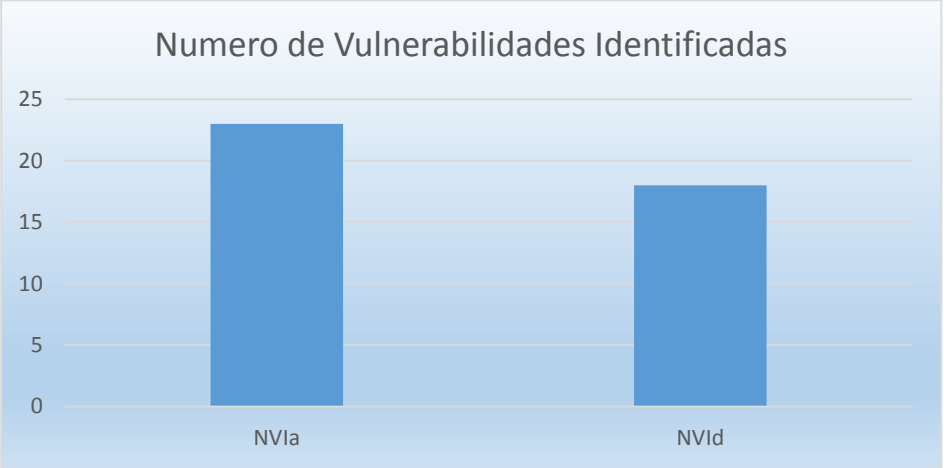
Tomando como única población la dirección IP publica de la infraestructura de Red de la Municipalidad Distrital de Víctor Larco Herrera se obtuvieron los siguientes resultados.

Tabla 7: Número de Vulnerabilidades Identificadas

Definición de Variables	**Resultados**
NVIa: Numero de Vulnerabilidades sin la Red Honeypot.	23
NIId: Numero de Vulnerabilidades con la Red Honeypot.	18
Diferencia	5

Fuente: Anexo N° 15. Informe de Vulnerabilidades
Elaboración: Microsoft Office Word 2016

Imagen 4: Numero de Vulnerabilidades Expuestas



Fuente: Informe de Vulnerabilidades (Anexo N° 15)
Elaboración: Microsoft Office Excel 2016.

3.1.3. Prueba de hipótesis para el indicador N° 03.

Numero de Intrusiones Identificadas

A. Definición de Variables:

NIIa: Numero de Intrusiones sin la Red Honeypot.

NIIp: Numero de Intrusiones con la Red Honeypot.

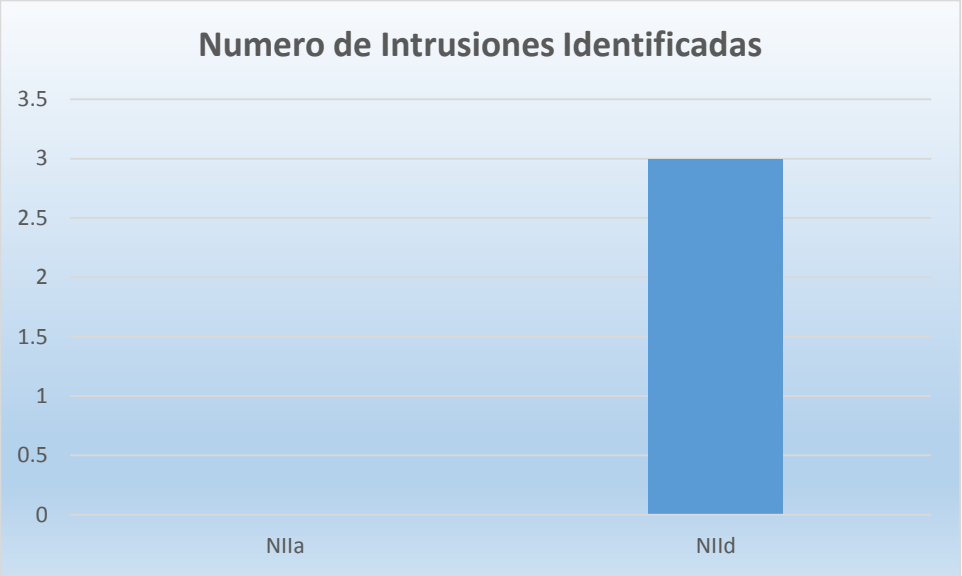
B. Resultados de la hipótesis. Tomando como única población la dirección IP publica de la infraestructura de Red de la Municipalidad Distrital de Víctor Larco Herrera se obtuvieron los siguientes resultados.

Tabla 8: Numero de Intrusiones Identificadas

Definición de Variables	**Resultados**
NIIa: Numero de Intrusiones Identificadas sin la Red Honeypot.	0
NII: Numero de Intrusiones Identificadas con la Red Honeypot	3
Diferencia	3

Fuente: Anexo N° XV. Informe de Vulnerabilidades
Elaboración: Microsoft Office Word 2016

Imagen 5: Numero de Intrusiones Identificadas



Fuente: Anexo N° XV. Reporte de Snort
Elaboración: Microsoft Office Word 2016

IV. DISCUSIÓN

La Municipalidad Distrital de Víctor Larco Herrera, como organismo de Gobierno Local promueve la participación de la ciudadanía brindando servicios públicos locales de alta calidad y para lo cual se basa de una infraestructura de Red, esencial para el cumplimiento de los distintos procesos que la Municipalidad realice. La infraestructura no contaba con herramientas que puedan detectar intrusiones, teniendo un índice de vulnerabilidad medio, por lo tanto, el uso de tecnologías como herramienta para la detección de intrusiones como es el desarrollo de una Red Honeypot para la detección de intrusiones, el análisis de la Infraestructura de Red, Detección de Intrusiones en Tiempo Real, la disminución de Vulnerabilidades y la disminución de Intrusiones en la Infraestructura de Red cumplió las expectativas de la municipalidad.
Se procedió a realizar distintas técnicas y herramientas de recolección de datos, para saber la problemática, dado a que no se encontró una metodología para el desarrollo de una Red Honeypot se consultó a expertos en el tema y validaron que se debía emplear la metodología de Hacking Ético.

En la fase I, Reconocimiento. Se realiza un análisis de la infraestructura de la red actual, indicador 1, presentado en la Imagen 2, se identifica el alcance y se recoleta información de manera pasiva y no intrusiva, luego se procedió el filtrado de información (footprinting)
Así mismo se elaboró el Diagrama donde se encuentra el Honeypot que se muestra en la Imagen 3; donde se establece que el Honeypot quedara fuera de la DMZ dada la complejidad y sensibilidad de esta zona (Quezada Torrez, 2014). En el análisis de viabilidad se obtuvo VAN S/. 3331.91 siendo el TIR 101%, por un tiempo de Recuperación de Capital de 11 meses y con 19 días.

En la fase II, Escaneo. En esta fase se identifican las vulnerabilidades, realizamos escaneos de red y de los puertos, con esto definimos los vectores de ataque, en esta fase a diferencia de (Wernher, y otros, 2016), no realizamos el escaneo del tráfico de los puertos, para determinar que Honeypot se implementara, sino que mediante el escaneo de las vulnerabilidades por parte de la herramienta OpenVas y Nmap, determinamos que el puerto 22/ssh, representa un numero de vulnerabilidades mayor que al resto de los puertos, es por eso que se toma esto como referencia para la elección de Kippo, un Honeypot bastante confiable que simula los servicios SSH.
Indicador II: El Número de vulnerabilidades de la Infraestructura de Red sin la Red Honeypot (Pre-Test), es de 23 y con la Red -Honeypot (Post-Test) es de 18, lo cual representa una

disminución de 5 vulnerabilidades encontradas. De tal manera en la investigación de (Wernher, y otros, 2016) solo implementan una Red Honeypot para mejorar la seguridad de los servidores logrando capturar información que haya sido recopilada por el Honeypot y en base a este se mejorara el sistema real, a diferencia del presente trabajo donde se identifican previamente las vulnerabilidades mediante pruebas de Hacking Ético lo cual representa una mejora considerable en base a estas pruebas se da la implementación de Kippo dado que el puerto 22 fueron identificadas la mayor parte de vulnerabilidades.

En la fase III, Obtener Acceso.

En esta fase aplicamos la validación y explotación de vulnerabilidades seguido de escalar los privilegios

Indicador III: Numero de Intrusiones en la Infraestructura de la Red sin la Red Honeypot (Pre-Test), es de 3 intrusiones y con la red Honeypot (Post-Test) es de 0 intrusiones, lo cual hay una disminución. Si comparamos con el trabajo realizado por (Dios Leon, y Ortiz Danae, 2014), en donde no se documenta intrusiones registradas, tenemos una gran diferencia con el trabajo de (Theodore, 2014), en donde el número de intrusiones es mayor en sistemas trampas con avisos en el que mostraban que la red estaba siendo monitoreada de las que no mostraban mensajes, pero si estaban siendo monitoreadas

En la fase IV, Mantener Acceso.

En esta Fase ya se ha logrado el acceso y el objetivo, es mantenernos con el acceso a la maquina víctima, instalamos puertas traseras (Backdoors), y elevación de privilegios (RootKit), en esta fase se hace el uso de herramientas como Metasploit, Meterpreter, Armitage, haciendo una comparación con los antecedentes previos, (Torres Quezada, 2014), utiliza la herramienta John in the Ripper para realizar ataques de fuerza bruta donde logra romper una de las claves pero no documenta si llega hacer uso de Backdoors, o si la cuenta que fue vulnerada presenta privilegios de administrador. En el dearrollo de esta esta investigacion se hace uso del exploit EternalBlue, asi como de sus variaciones, estos exploits fueron publicados por el grupo denominado The Shadow Brokers, quienes fueron los que sustrayeron de los servidores de la NSA, esto nos permitio tener acceso remoto a traves de una shell System.

V. CONCLUSIONES

1. Se consiguió mejorar la detección de intrusiones con el desarrollo de una Red Honeypot en la infraestructura de Red de la Municipalidad Distrital de Víctor Larco Herrera, siendo económicamente factible al estudio elaborado obteniendo una ganancia de s/0.01, logrando obtener ganancias de 16% hasta el cuarto año.

2. Se logró realizar el análisis de la Infraestructura de Red obteniendo el diseño lógico de la infraestructura de red.

3. Se logró disminuir el número de vulnerabilidades de la Infraestructura de Red de la Municipalidad Distrital de Víctor Larco, disminuyendo las vulnerabilidades con calificación de riesgo alto de 5 a 0 vulnerabilidades, habiendo encontrado un total de 23 vulnerabilidades antes del desarrollo de la Red Honeypot, se redujo 21.7%

4. Se logró determinar el número de intrusiones en la Infraestructura de Red de la Municipalidad, logrando detectar el 100% de intrusiones.

5. Se concluye que el desarrollo de la Red Honeypot para la detección de intrusiones es económicamente factible, de acuerdo con el estudio elaborado; como resultado tenemos que por una inversión de cada sol obtendremos por cada sol invertido obtendremos s/0.01 de ganancia, siendo el TIR de 16% y teniendo un lapso de Retorno de Capital de 11 meses, 19 días.

VI. RECOMENDACIONES

A la Subgerencia de Tecnologías de Información:

1. Se recomienda mejorar el nivel de seguridad ante intrusiones y o ataques con el desarrollo de Sistemas de Prevención de Intrusiones IPS

2. Se recomienda tener actualizada la información con respecto a los cambios realizados en la infraestructura de red de la Municipalidad

3. Se recomienda pruebas de Pentesting sobre el entorno web y análisis forense sobre las aplicaciones web para obtener un mayor detalle de posibles nuevas vulnerabilidades que no hayan sido detectadas en este trabajo

4. Se recomienda la implementación de más Honeypots que simulen la Infraestructura de Red por completo, logrando tener un mayor campo de vigilancia sobre ataques y la aplicación de estos en la DMZ como en la LAN.

5. Se recomienda la aplicación de políticas de seguridad más proactivas, la implementación y cumplimiento de la ISO 27000 así como también la aplicación de estrategias como el cubo de McCumber.

6. La capacitación y retroalimentación constante al personal sobre temas relacionados con Ciberseguridad, exponerlos ante ataque es una manera de que ellos tomen conciencia sobre el peligro latente y lo expuestos que están, siendo el personal el eslabón más débil.

Referencias

Academy, Cisco Networking. 2017. www.netacad.com. *Netacad.* [En línea] 2017. [Citado el: 05 de 05 de 2018.] https://static-course-assets.s3.amazonaws.com/CyberSec2/es/index.html#1.1.1.1.

Avast, Software. avast software, inc. [En línea] [Citado el: 14 de 05 de 2018.] https://www.avast.com/es-es/c-zero-day.

Bakinter, Fundacion Innovacion. 2015. www.fundacionbakinter.org. [En línea] 2015. [Citado el: 30 de 09 de 2017.] Prologo de Eden Shochat. https://www.fundacionbankinter.org/documents/20183/137030/CS_COMPLETO_ESP_2016.pdf/a3cad692-9d29-4602-90db-1718d17ca418.

Barbieri, Leonardo. 2015. ITWARE LATAM. [En línea] 16 de 10 de 2015. [Citado el: 02 de 10 de 2017.] http://www.itwarelatam.com/2014/10/16/las-tendencias-en-seguridad-que-marcaran-el-2015/.

Cameron Camp y Stephen Cobb. 2017. *La Seguridad como Rehen.* Eset. 2017. Pag. 41.

DHS, Deparment of Homeland Security. 2013. Deparment of Homeland Security. [En línea] 13 de 02 de 2013. [Citado el: 01 de 10 de 2017.] Critical Infrastructure Security and Resilience. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Dios Leon, Saby Yasmith y Ortiz Leon, Danae Alicia. 2014. Universidad Nacional Trujillo. [En línea] 03 de 2014. [Citado el: 25 de 09 de 2017.] http://www.inf.unitru.edu.pe/revista/6.pdf.

Empresarial, Business. 2017. http://www.businessempresarial.com.pe. [En línea] 14 de 08 de 2017. [Citado el: 02 de 10 de 2017.] http://www.businessempresarial.com.pe/peru-registra-usd-4-mil-782-millones-de-dolares-en-perdidas-por-cibercrimen/.

Gabriel, Bergel. 2016. Metodologias de testing de seguridad. *#11PathsTalks: metodologías testing de seguridad.* s.l. : ElevenPaths, 11 de 04 de 2016.

government, HM. 2016. *National Cyber Security Strategy.* Cabinet Office, National security and intelligence, HM Treasury, and The Rt Hon Philip Hammond MP . Londres : s.n., 2016. pág. 80, Documento Politico. Anexo 1: Acronimos.

Gupta, Pritesh. 2005. El portal de ISO 27001 en Español. [En línea] 2005. [Citado el: 26 de 09 de 2017.] http://www.iso27000.es/sgsi.html.

KnowBe4, Inc. Phishing.org. [En línea] [Citado el: 13 de 05 de 2018.] http://www.phishing.org/phishing-and-spoofing.

MIT. 2005. Instituto Tecnológico de Massachusetts - MIT. [En línea] Red Hat, Inc., 2005. [Citado el: 02 de 11 de 2017.] ISBN: N/A. http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html.

Observatorio de la Ciberseguridad en America Latina. 2016. *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? .* Banco Interamericano de Desarrollo & Organizacion de los Estados Americanos. 2016. Informe de Ciberseguridad.

Quezada Torrez, Rebeca Soledad. 2014. UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE. [En línea] 21 de 01 de 2014. [Citado el: 20 de 09 de 2017.] https://repositorio.espe.edu.ec/bitstream/21000/10470/1/T-ESPE-048394.pdf.

Report, MENA. 2016. search.proquest.com. *ProQuest Central.* [En línea] 19 de 02 de 2016. [Citado el: 12 de 05 de 2018.] https://search.proquest.com/docview/1766963728?accountid=37408.

Russell Pinto, de Oliveira DIaz. 2014. http://repositorio.unapiquitos.edu.pe. [En línea] 2014. [Citado el: 15 de 09 de 2017.] http://repositorio.unapiquitos.edu.pe/handle/UNAP/4489.

Samaniego, Felix. 2017. *Fabulas en verso castellano para el uso del Real Seminario Vascongado.* s.l. : Red ediciones, 2017. Fabula XI, Pag 27. 978-84-9887-749-9.

Spitzner, lance. 2002. *Honeypots: Tracking Hackers.* Boston : Addison Wesley, 2002. pág. 408. Pag. 62. 0-321-10895-7.

Spitzner, Lancer. 2002. *Honeypots: Tracking Hackers.* Boston : Addison Wesley, 2002. pág. 480. Pag. 54. ISBN: 0-321-10895-7.

Theodore, Henry Wilson II. 2014. University the Maryland. *University the Maryland Web site.* [En línea] 2014. [Citado el: 20 de 03 de 2018.] https://drum.lib.umd.edu/bitstream/handle/1903/15238/WilsonII_umd_0117N_15034.pdf;sequence=1.

Vlajic, N. 2013. Electric Engineering and computer Science. [En línea] 2013. [Citado el: 12 de 05 de 2018.] https://www.eecs.yorku.ca/course_archive/2013-14/F/4482/CSE4482_01_Introduction_2013_posted.pdf.

Wernher, Raul y Nuñez, Aragon. 2016. repositorio.uandina.edu.pe. [En línea] 2016. [Citado el: 26 de 09 de 2017.] http://repositorio.uandina.edu.pe/bitstream/UAC/753/1/RESUMEN.pdf.

Zink, Terry. 2009. blogs.msdn.microsoft.com. [En línea] 29 de 08 de 2009. [Citado el: 14 de 05 de 2018.] blogs.msdn.microsoft.com.

Anexos

Anexo 01 Carta de Aceptación de desarrollo de institución

MUNICIPALIDAD DISTRITAL DE VÍCTOR LARCO HERRERA
TRUJILLO – PERÚ

CARTA DE ACEPTACIÓN

Víctor Larco Herrera, 17 de Junio de 2018

De: Ing. Yony Salome Vera Toledo
Subgerente de Tecnologías de Información

A: Dr. Juan Francisco pacheco Torres
Director De La Escuela Profesional de Ingeniería de Sistemas

Por el medio del presente me dirijo a usted con la finalidad de informarle que la "**Subgerencia de Tecnologías de Información de la Municipalidad Distrital de Víctor Larco Herrera"** acepta el desarrollo del Proyecto de Investigación **"Desarrollo de una Red Honeypot para la Detección de Intrusiones en la Municipalidad de Víctor Larco Herrera - Trujillo"** realizado por el **Sr. Valdiviezo Avalo Jormy Jean Franco,** identificado con **DNI 70411699**, estudiante del X ciclo de la escuela profesional de Ingeniería de Sistemas de la Universidad Cesar Vallejo, habiendo realizado un importante aporte en mejorar la seguridad de la Infraestructura de Red ante futuras intrusiones.

Se expide la presente carta a solicitud de la parte interesada para los fines que convengan

MUNICIPALIDAD DISTRITAL "VÍCTOR LARCO HERRERA"
Ingº YONY S. VERA TOLEDO
Sub Gerente de Tecnología de la Información

Anexo 02: Lluvia de Ideas

- ✓ Demora en la realización de reportes de intrusiones.
- ✓ Falta de Herramientas que permitan la detección de intrusiones reportes de intrusiones a la infraestructura de red.
- ✓ Falta de registros de intrusiones agrupadas ni organizadas falta de personal encargado en monitorear intrusiones
- ✓ No existe un plan de contingencia ante intrusiones No existe un Plan de respuestas ante intrusiones
- ✓ Desconocimiento de los tipos de intrusiones más usados

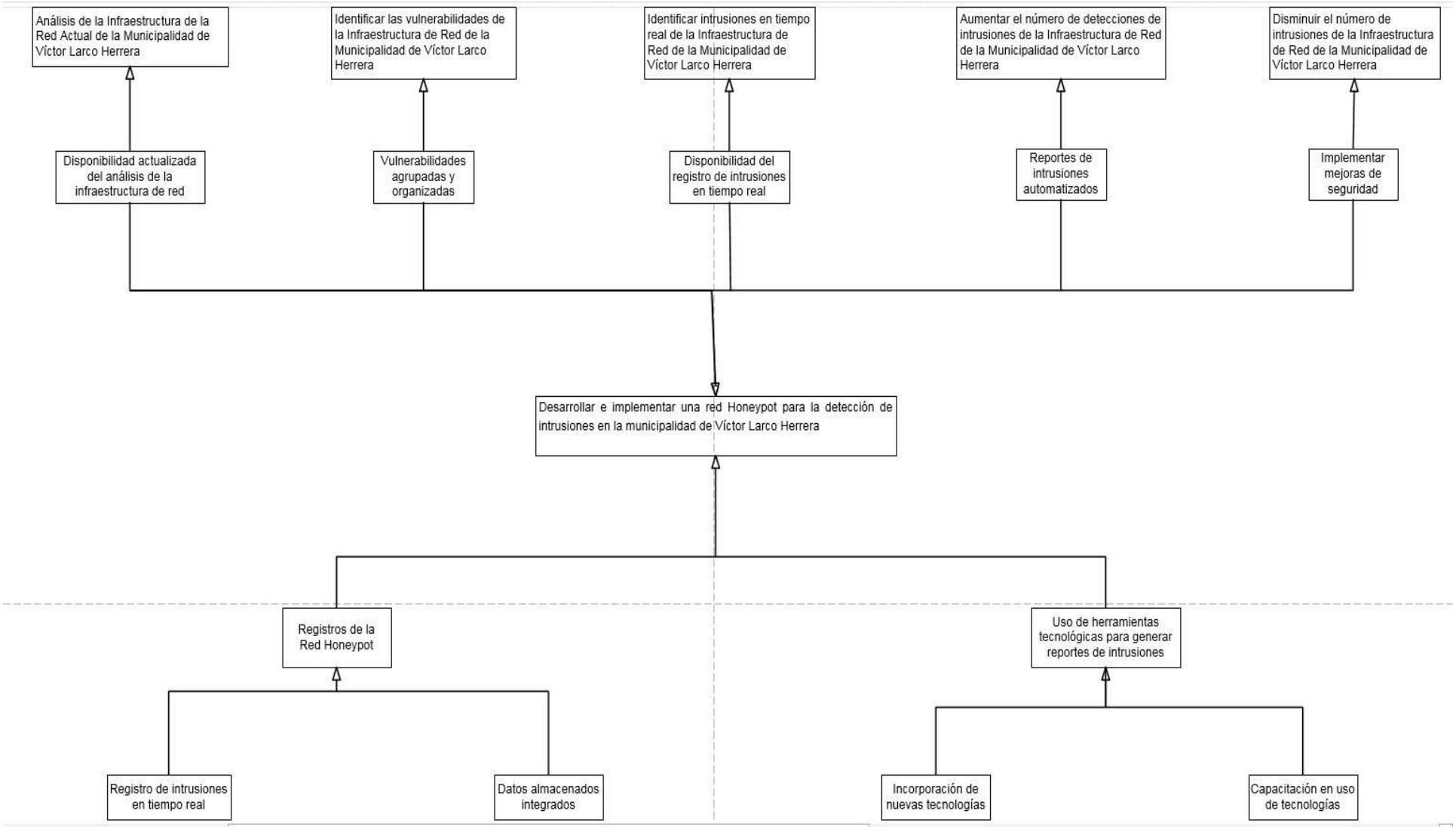
Anexo 03: Tabla de frecuencia

CAUSAS	Frecuencia	Frec. Normaliz
Demora en la realización de reportes de intrusiones	25	45%
Falta de Herramientas que permitan la detección de intrusiones	2	4%
Reportes de intrusiones a la infraestructura de red	19	35%
Falta de registros de intrusiones agrupadas ni organizadas	2	4%
Falta de personal encargado en monitorear intrusiones	2	4%
No existe un plan de contingencia ante intrusiones	1	2%
No existe un Plan de respuestas ante intrusiones	1	2%
Desconocimiento de los tipos de intrusiones más usadas	2	4%
	TOTAL	**100%**

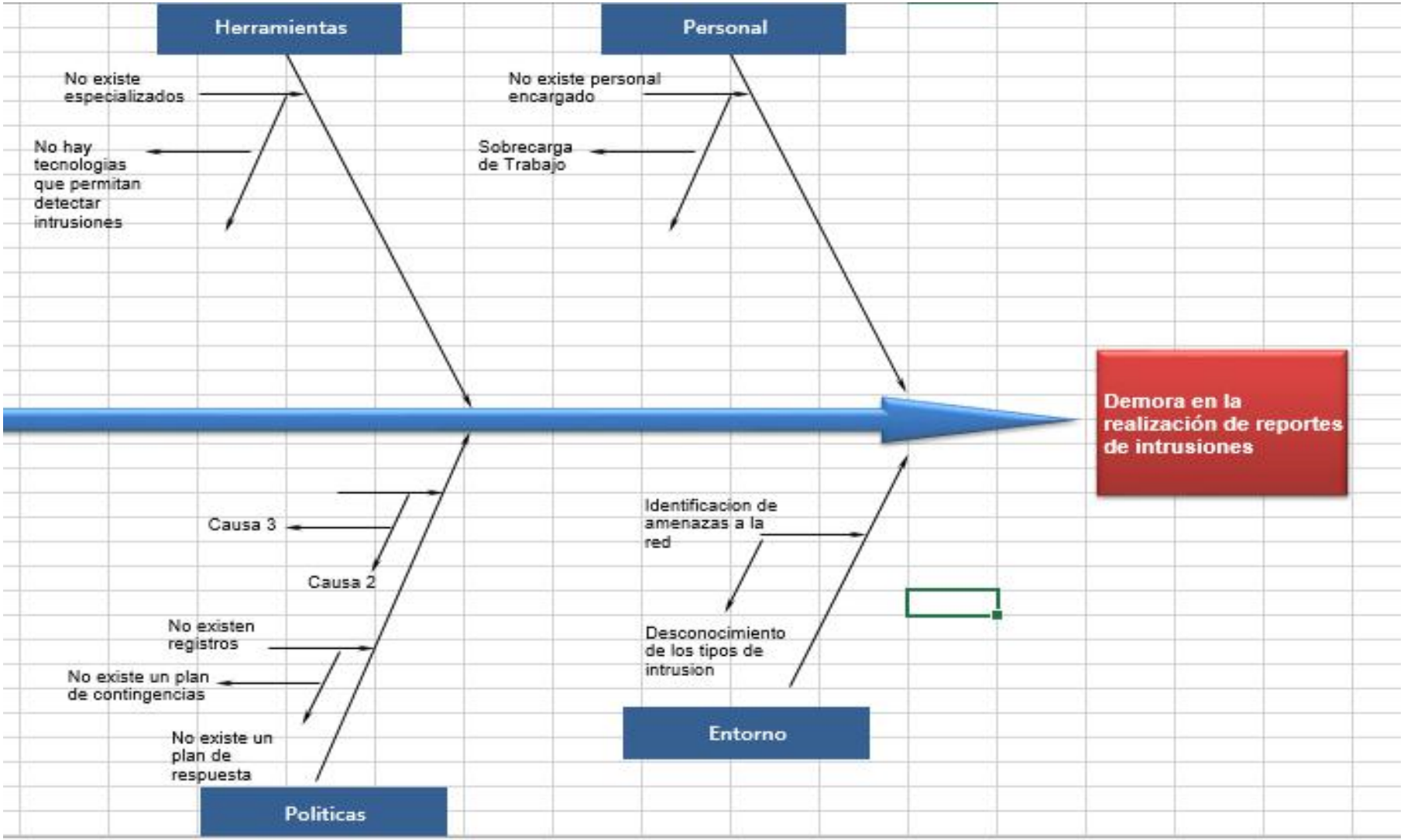
Anexo 04: Tabla de Frecuencias Ordenadas

CAUSAS	Frecuencia	Frec. Normaliz	Frec.
Demora en la realización de reportes de intrusiones	25	45%	45%
Falta de Herramientas que permitan la detección	19	35%	80%
Reportes de intrusiones a la infraestructura de red	2	4%	84%
Falta de registros de intrusiones agrupadas ni	2	4%	87%
Falta de personal encargado en monitorear	2	4%	91%
No existe un plan de contingencia ante	2	4%	95%
No existe un Plan de respuestas ante intrusiones	1	2%	96%
Desconocimiento de los tipos de intrusiones más usados	1	2%	98%
Demora en la realización de reportes de intrusiones	1	2%	100%
		TOTAL	**100%**

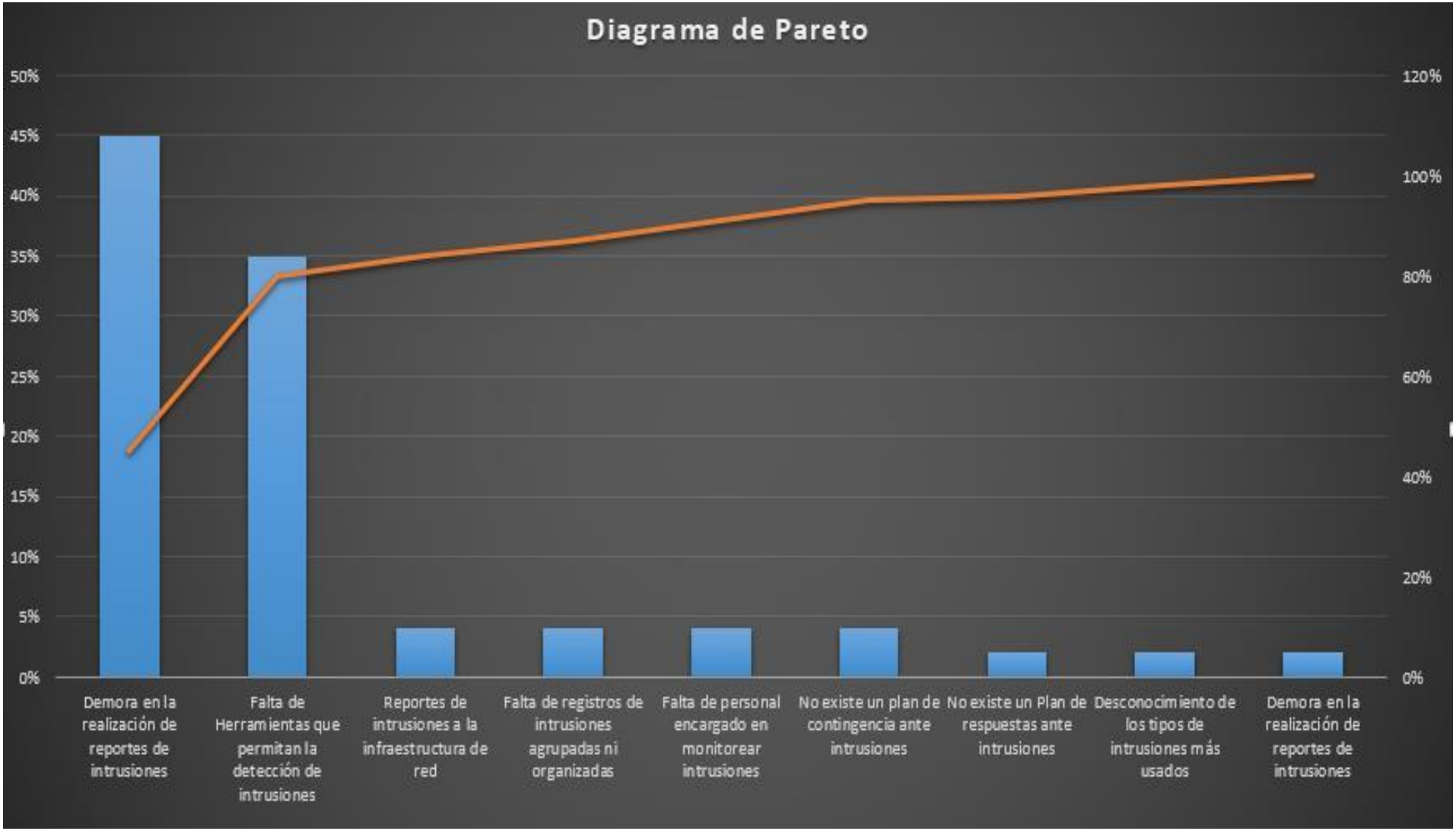
Anexo 05: Árbol de Objetivos



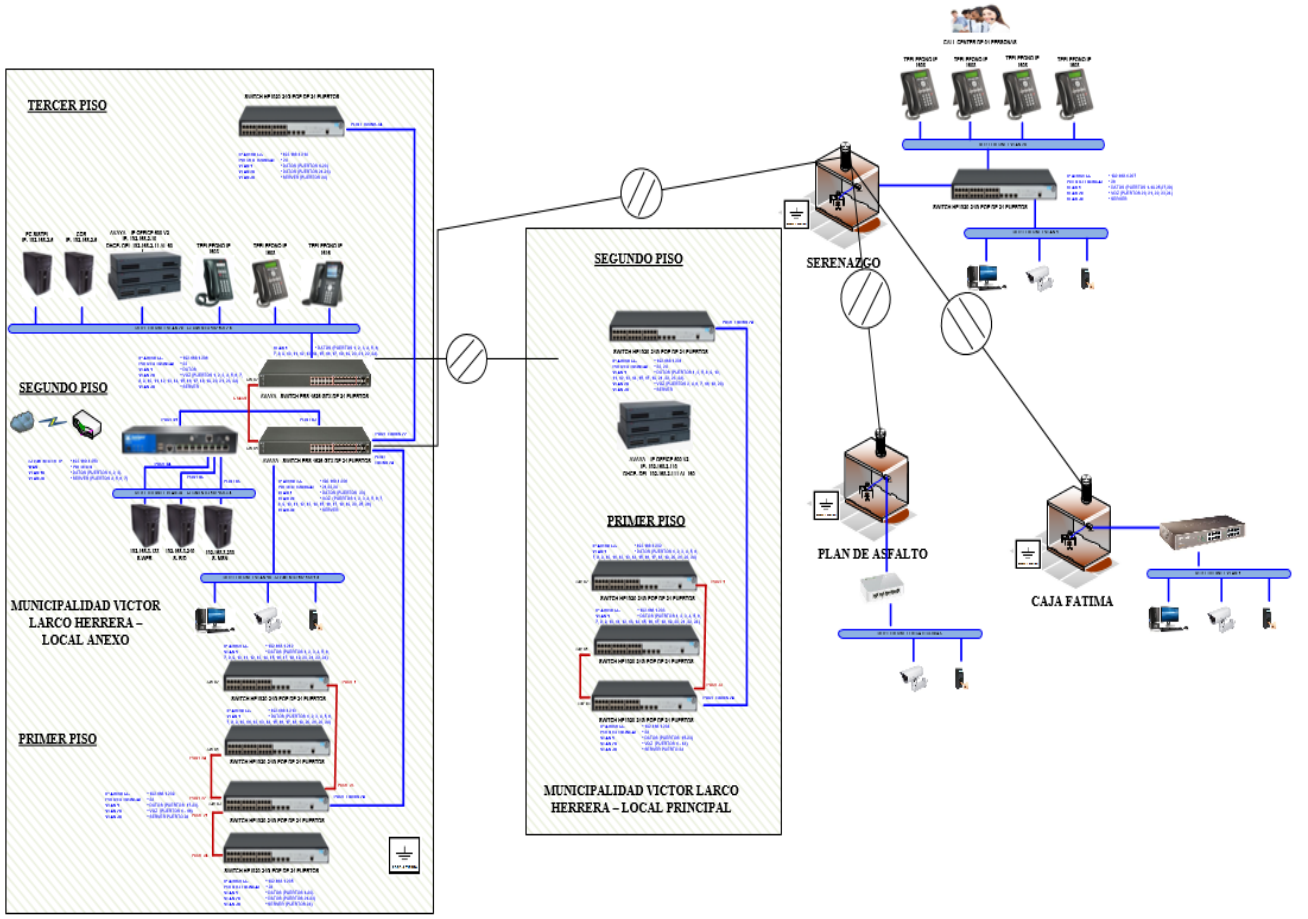
Anexo 06: Espina de Ishikawa



Anexo 07: Diagrama de Pareto

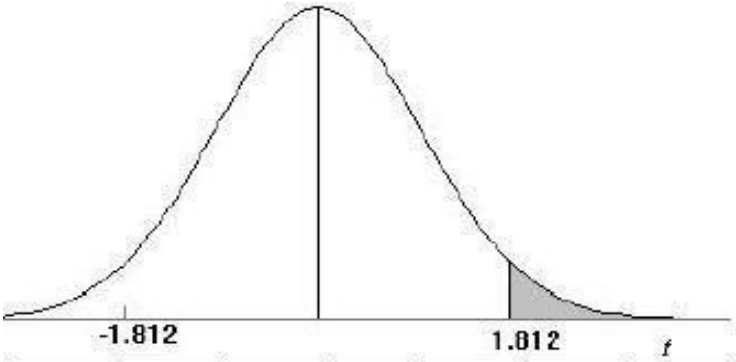


Anexo 08: Esquema general del diseño lógico de la infraestructura de red



Elaboración: Microsoft Office Word 2016.

Anexo 09: Tabla de Distribución Normal Z



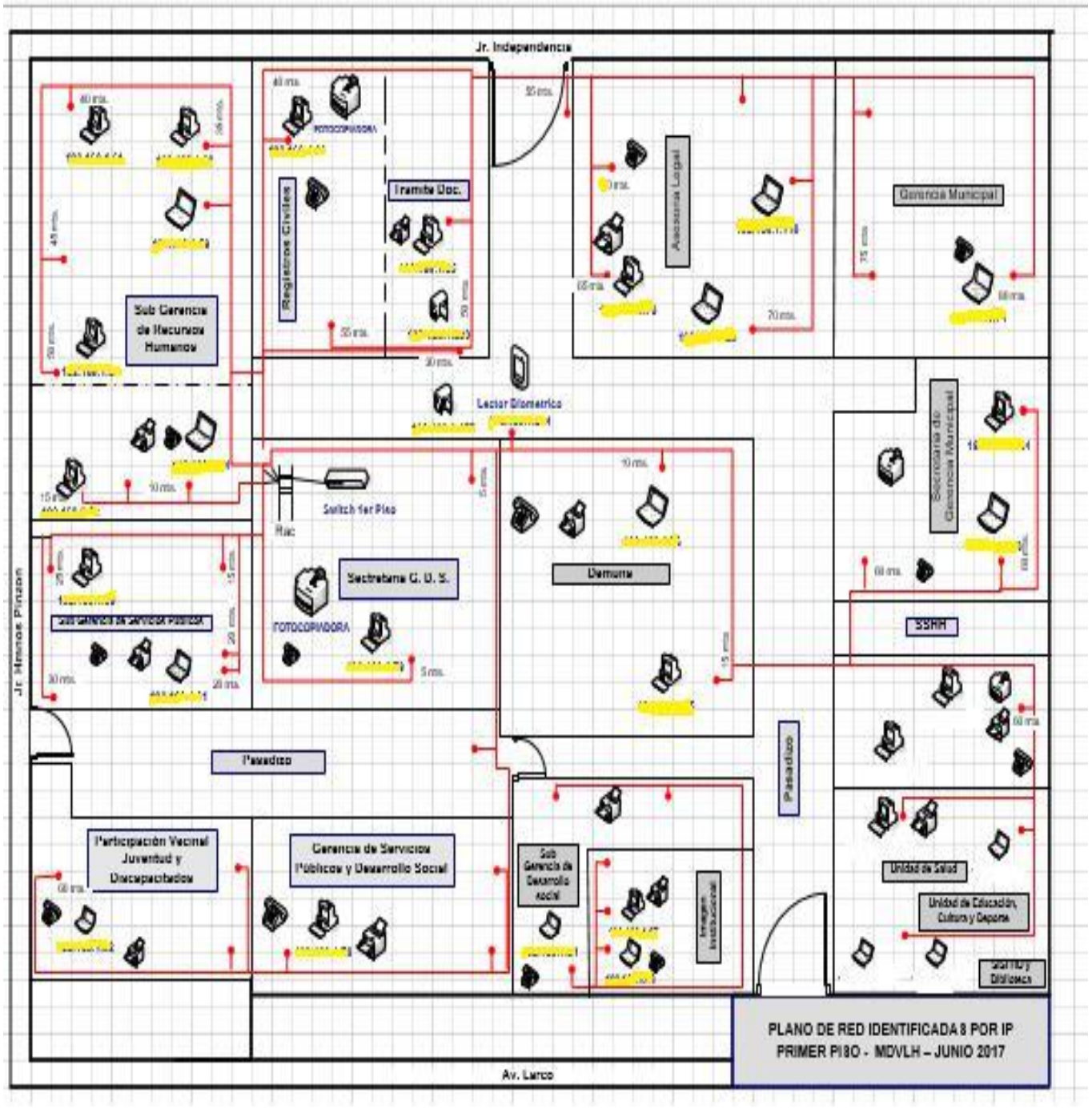
Ejemplo

Para r = 10 grados de libertad:

P[t > 1.812] = 0.05
P[t < -1.812] = 0.05

r \ α	0,25	0,2	0,15	0,1	0,05	0,025	0,01	0,005	0,0005
1	1,000	1,376	1,963	3,078	6,314	12,706	31,821	63,656	636,578
2	0,816	1,061	1,386	1,886	2,920	4,303	6,965	9,925	31,600
3	0,765	0,978	1,250	1,638	2,353	3,182	4,541	5,841	12,924
4	0,741	0,941	1,190	1,533	2,132	2,776	3,747	4,604	8,610
5	0,727	0,920	1,156	1,476	2,015	2,571	3,365	4,032	6,869
6	0,718	0,906	1,134	1,440	1,943	2,447	3,143	3,707	5,959
7	0,711	0,896	1,119	1,415	1,895	2,365	2,998	3,499	5,408
8	0,706	0,889	1,108	1,397	1,860	2,306	2,896	3,355	5,041
9	0,703	0,883	1,100	1,383	1,833	2,262	2,821	3,250	4,781
10	0,700	0,879	1,093	1,372	1,812	2,228	2,764	3,169	4,587
11	0,697	0,876	1,088	1,363	1,796	2,201	2,718	3,106	4,437
12	0,695	0,873	1,083	1,356	1,782	2,179	2,681	3,055	4,318
13	0,694	0,870	1,079	1,350	1,771	2,160	2,650	3,012	4,221
14	0,692	0,868	1,076	1,345	1,761	2,145	2,624	2,977	4,140
15	0,691	0,866	1,074	1,341	1,753	2,131	2,602	2,947	4,073
16	0,690	0,865	1,071	1,337	1,746	2,120	2,583	2,921	4,015
17	0,689	0,863	1,069	1,333	1,740	2,110	2,567	2,898	3,965
18	0,688	0,862	1,067	1,330	1,734	2,101	2,552	2,878	3,922
19	0,688	0,861	1,066	1,328	1,729	2,093	2,539	2,861	3,883
20	0,687	0,860	1,064	1,325	1,725	2,086	2,528	2,845	3,850
21	0,686	0,859	1,063	1,323	1,721	2,080	2,518	2,831	3,819
22	0,686	0,858	1,061	1,321	1,717	2,074	2,508	2,819	3,792
23	0,685	0,858	1,060	1,319	1,714	2,069	2,500	2,807	3,768
24	0,685	0,857	1,059	1,318	1,711	2,064	2,492	2,797	3,745
25	0,684	0,856	1,058	1,316	1,708	2,060	2,485	2,787	3,725
26	0,684	0,856	1,058	1,315	1,706	2,056	2,479	2,779	3,707
27	0,684	0,855	1,057	1,314	1,703	2,052	2,473	2,771	3,689
28	0,683	0,855	1,056	1,313	1,701	2,048	2,467	2,763	3,674
29	0,683	0,854	1,055	1,311	1,699	2,045	2,462	2,756	3,660
30	0,683	0,854	1,055	1,310	1,697	2,042	2,457	2,750	3,646
40	0,681	0,851	1,050	1,303	1,684	2,021	2,423	2,704	3,551
60	0,679	0,848	1,045	1,296	1,671	2,000	2,390	2,660	3,460
120	0,677	0,845	1,041	1,289	1,658	1,980	2,358	2,617	3,373
∞	0,674	0,842	1,036	1,282	1,645	1,960	2,326	2,576	3,290

Anexo 10: Plano de Red Identificada por IP primer piso



Anexo 11: Plantilla para la elección de la metodología de desarrollo Metodólogo *1*

Anexo 10: Formato para la elección de la metodología de desarrollo

ENCUESTA A EXPERTOS PARA LA SELECCIÓN DE METODOLOGÍA

Objetivo Reunir información esencial para la selección de la metodología a aplicar en el desarrollo de la tesis.

Dirigido a: Profesionales con experiencia en metodologías de desarrollo para la elaboración de la tesis

1. **Nombres y Apellidos:** EDWIN MENDOZA TORRES
2. **Generalidades:**

Profesión

Ingeniero de Sistemas ( ) Ingeniero Informático (X)

Ingeniero de Software ( ) Otro ( )

Años de Experiencia

1-5 años ( ) 5-10 años ( ) 10 a más años (X)

Especialidad

Desarrollo de Software ( )

Auditoria de Sistemas y Seguridad e la Información ( )

Sistemas y Tecnologías de la Información (X)

Otro ( ) Especificar: _____

Para la adición de la puntuación se seguirá la siguiente escala de Valorización:

Valoración	Escala
Pésimo	1
Malo	2
Regular	3
Bueno	4
Excelente	5

Metodologías Expuestas

PPDIOO – CISCO: Se definen las actividades necesarias en cada fase del ciclo de vida de la red. Está enfocado en definir las mínimas actividades requeridas por tecnología y complejidad de red.

Fases: Preparación, Planeación, Diseño, Implementación, Operación y Optimización (PPDIOO)

Top-Down Network Design: Se identifican las metas y necesidades del negocio, trabajando con el cliente para desarrollar un análisis de retorno de inversión.
Fases: Análisis de Requerimientos, Desarrollo del Diseño Lógico, Desarrollo del Diseño Físico, Pruebas, Optimización, Documentación del Diseño

OSSTMM: Manual de la Metodología Abierta de Comprobación de la Seguridad, es un protocolo de auditoria de seguridad y se centra en los detalles técnicos que deben tenerse en cuenta antes, durante y después de una prueba de seguridad
Fases: Seguridad de la Información, Seguridad de los Procesos, Seguridad en las tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica, Seguridad Física.

Calificación de la Metodología de acuerdo a criterio Escala de Valorización:

Criterios	OSSTMM	PPDIO O-Cisco	HACKING ETHICAL
Flexibilidad	2	3	3
Información	4	4	4
Compatibilidad	1	2	4
Costo de Desarrollo	3	3	3
Tiempo de Desarrollo	3	2	4
Herramientas a medida	1	3	5
Simplicidad	2	2	4
Iniciación	3	3	4
Elaboración	2	2	3
Participación del cliente	4	2	5
Facilidad de uso	4	3	4
Iniciación	3	2	4
Construcción	3	2	3
Transición	2	3	4
Pruebas	2	3	5
TOTAL:	39	39	69

Juan Carlos Huamán Cueva
INGENIERO DE SISTEMAS
REG CIP 134739

Anexo 12: Plantilla para la elección de la metodología de desarrollo Especialista 2

Anexo 10: Formato para la elección de la metodología de desarrollo

ENCUESTA A EXPERTOS PARA LA SELECCIÓN DE METODOLOGÍA

Objetivo Reunir información esencial para la selección de la metodología a aplicar en el desarrollo de la tesis.

Dirigido a: Profesionales con experiencia en metodologías de desarrollo para la elaboración de la tesis

1. **Nombres y Apellidos:** JUAN C. HUAMAN CUEVA
2. **Generalidades:**

Profesión

Ingeniero de Sistemas (X) Ingeniero Informático ( )

Ingeniero de Software ( ) Otro ( )

Años de Experiencia

1-5 años ( ) 5-10 años (X) 10 a más años ( )

Especialidad

Desarrollo de Software ( )

Auditoria de Sistemas y Seguridad e la Información ( )

Sistemas y Tecnologías de la Información (X)

Otro ( ) Especificar: _____

Para la adición de la puntuación se seguirá la siguiente escala de Valorización:

Valoración	Escala
Pésimo	1
Malo	2
Regular	3
Bueno	4
Excelente	5

Metodologías Expuestas

PPDIOO – CISCO: Se definen las actividades necesarias en cada fase del ciclo de vida de la red. Está enfocado en definir las mínimas actividades requeridas por tecnología y complejidad de red.

Fases: Preparación, Planeación, Diseño, Implementación, Operación y Optimización (PPDIOO)

Top-Down Network Design: Se identifican las metas y necesidades del negocio, trabajando con el cliente para desarrollar un análisis de retorno de inversión.
Fases: Análisis de Requerimientos, Desarrollo del Diseño Lógico, Desarrollo del Diseño Físico, Pruebas, Optimización, Documentación del Diseño

OSSTMM: Manual de la Metodología Abierta de Comprobación de la Seguridad, es un protocolo de auditoria de seguridad y se centra en los detalles técnicos que deben tenerse en cuenta antes, durante y después de una prueba de seguridad
Fases: Seguridad de la Información, Seguridad de los Procesos, Seguridad en las tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica, Seguridad Física.

Calificación de la Metodología de acuerdo a criterio Escala de Valorización:

Criterios	OSSTMM	PPDIO O-Cisco	HACKING ETHICAL
Flexibilidad	2	3	3
Información	4	4	4
Compatibilidad	1	2	4
Costo de Desarrollo	3	3	3
Tiempo de Desarrollo	3	2	4
Herramientas a medida	1	3	5
Simplicidad	2	2	4
Iniciación	3	3	4
Elaboración	2	2	3
Participación del cliente	4	2	5
Facilidad de uso	4	3	4
Iniciación	3	2	4
Construcción	3	2	3
Transición	2	3	4
Pruebas	2	3	5
TOTAL:	39	39	69

Juan Carlos Huamán Cueva
INGENIERO DE SISTEMAS
REG CIP 134739

Anexo 13: Plantilla para la elección de la metodología de desarrollo Especialista 3

UCV UNIVERSIDAD CÉSAR VALLEJO

PLANTILLAS PARA LA EVALUACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

1. IDENTIFICACION DEL EXPERTO

NOMBRE DEL EXPERTO: EDWIN MENDOZA TORRES

DNI_____ PROFESION: INGENIERO INFORMATICO

LUGAR DE TRABAJO: UNIVERSIDAD CESAR VALLEJO

CARGO QUE DESEMPEÑA: DOCENTE

DIRECCION: _____

TELEFONO FIJO: _____ MOVIL: _____

DIRECCION ELECTRONICA: EMENDOZATORRES @ gmail.com

FECHA DE EVALUACIÓN: 21-11-17

FIRMA DEL EXPERTO: _____

EDWIN R. MENDOZA TORRES
ING. INFORMATICO
REG. CIP. 75445

2. PLANILLA DE VALIDACION DEL INSTRUMENTO

CRITERIOS	APRECIACION CUALITATIVA			
	EXCELENTE (4)	BUENO (3)	REGULAR (2)	DEFICIENTE (1)
Presentación del instrumento		X		
Claridad en la redacción de los ítems		X		
Pertinencia de las variables con los indicadores			X	
Relevancia del contenido		X		
Factibilidad de la aplicación	X			

APRECIACION CUALITATIVA: _____

OBSERVACIONES: _____

3. **JUICIO DE EXPERTOS:**

- En líneas generales, considera Ud. que los indicadores de las variables están inmersos en su contexto teórico de forma:

SUFICIENTE X	MEDIANAMENTE SUFICIENTE	INSUFICIENTE

OBSERVACION:

_____
_____
_____
_____

- Considera que los reactivos del cuestionario miden los indicadores seleccionados para la variable de manera:

SUFICIENTE	MEDIANAMENTE SUFICIENTE X	INSUFICIENTE

OBSERVACION:

_____
_____
_____
_____

- El instrumento diseñado mide la variable de manera:

SUFICIENTE	MEDIANAMENTE SUFICIENTE X	INSUFICIENTE

OBSERVACION:

_____
_____
_____
_____

- El instrumento diseñado es:

_____
_____
_____
_____

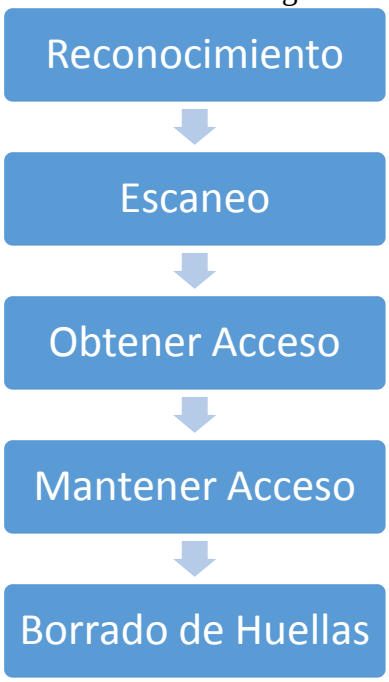
Anexo 14: Metodología de Hacking Ético

METODOLOGÍA DE HACKING ÉTICO

Es una de las metodologías más aplicadas por expertos en seguridad de la información a la función que cumplen los profesionales en seguridad de la información, estos utilizan sus conocimientos de hacking con fines defensivos, su función es de determinar las acciones que puede realizar un atacante en contra de un sistema de información.

El desarrollo del siguiente proyecto se limitará a las tres primeras fases de la metodología de Hacking Ético las últimas dos fases no serán tomadas, dado que la fase de mantener acceso se obviaría ya que el exploit utilizado nos proporciona directamente una puerta trasera (backdoor) y la última fase de borrado de huellas a pesar de que no se necesitan conocimientos avanzados para ocultarse o borrar información de registros a través de diferentes métodos y herramientas, si se necesitan conocimientos avanzados en cómo evitar lo mencionado anteriormente, y por la naturaleza del proyecto que es de demostrar que la Infraestructura de Red ha sido afectada por lo cual es necesario dejar registros para su validación y estudios posteriores.

Imagen 6: Fases de la Metodología de Hacking Ético



Fuente: Anexo 14, .
Elaboración: Microsoft Office Word 2016.

Fases De Hacking Ético

1. **Reconocimiento**
   - Identificamos el alcance
   - Recolectamos información de manera pasiva y no intrusiva
   - Hacemos uso del Framework OSINT como referencia

Herramientas usadas:

- ✓ Foca Open Source.
- ✓ Maltego

Realizamos análisis de los metadatos de todos los archivos que están publicados en el dominio de la Municipalidad.

Total, de Archivos examinados: 100
Usuarios encontrados: 8
Sistema Operativo: 1
Dominio: munivictorlarco.gob.pe

Imagen 7: Usuarios encontrados

Attribute	Value
All users found (8) - Times found	
Name	BERNARDO TORIBIO
Name	CENTRAL
Name	SGTI-LT
Name	CENTRAL
Name	Wordcraft International Limited
Name	Felipe Andr?s Mart?nez Suyo
Name	USUARIO
Name	Diego Stahl Huaman Rios

Fuente: FOCA Open Source 3.4
Elaboración: Microsoft Office Word 2016.

Imagen 8: SO encontrados

Attribute	Value
Information	
Name	PC_CENTRAL
Operating System	Windows Vista

Fuente: FOCA Open Source 3.4
Elaboración: Microsoft Office Word 2016.

- Realizamos un escaneo del dominio para identificar el mapa de subdominios.

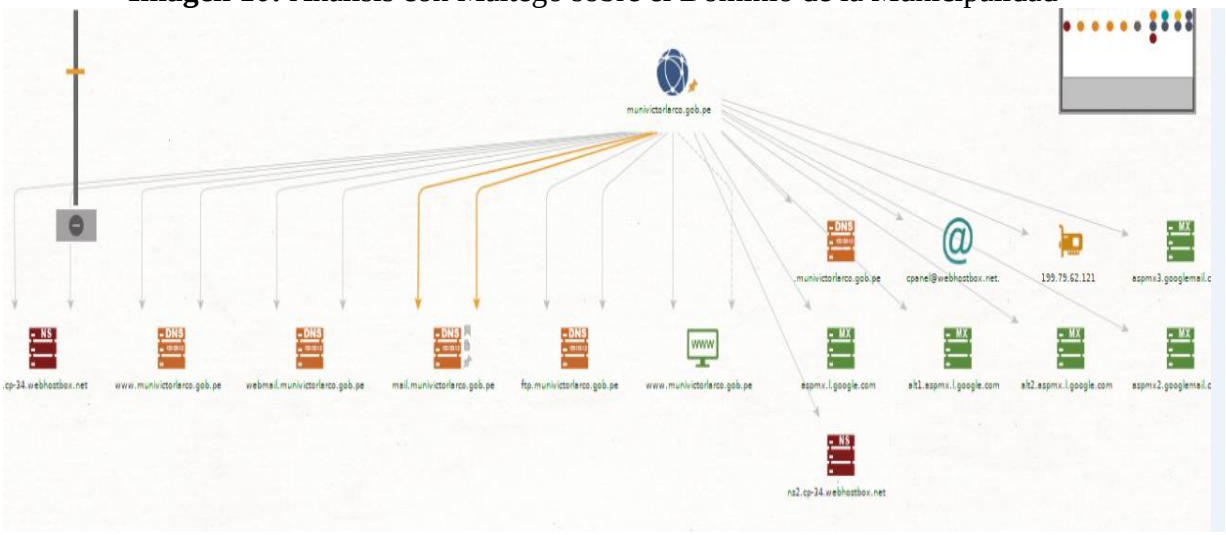
Imagen 9: Subdominios

Time	Source	Severity	Message
16:06:11	DNSCommonNa	medium	[199.79.62.121] Found subdomain mail.munivictorlarco.gob.pe
16:06:11	DNSCommonNa	medium	[199.79.62.121] Found subdomain www.munivictorlarco.gob.pe
16:06:11	DNSCommonNa	medium	[199.79.62.121] Found subdomain webmail.munivictorlarco.gob.pe
16:06:12	DNSCommonNa	medium	[199.79.62.121] Found subdomain ftp.munivictorlarco.gob.pe
16:06:33	DNSCommonNa	medium	[199.79.62.121] Found subdomain cpanel.munivictorlarco.gob.pe
16:08:19	DNSCommonNa	medium	[199.79.62.121] Found subdomain localhost.munivictorlarco.gob.pe

Fuente: FOCA Open Source 3.4.
Elaboración: Microsoft Office Word 2016.

- Hacemos uso de Maltego, este software nos permite aplicar análisis forense para la búsqueda de información de fuentes abiertas, logrando visualizar en un entorno gráfico, para aplicar análisis de enlaces y minería de datos, creando entidades personalizadas; Maltego realiza una búsqueda de registros DNS, registros de whois, motores de búsqueda, redes sociales en línea, además de Varias APIs en línea y de Metadatos.

Imagen 10: Análisis con Maltego sobre el Dominio de la Municipalidad



Fuente: Maltego CE.
Elaboración: Microsoft Office Word 2016.

2. Escaneo

- Identificamos las vulnerabilidades
- Realizamos el escaneo de red y puertos haciendo uso de la herramienta Nmap.
- Definir vectores de ataques

Herramientas usadas:

- ✓ Nmap /Zenmap
- ✓ Ftester
- ✓ Brutus
- ✓ Maltego
- ✓ TFTP; BruteForce.

Imagen 11: Escaneo Nmap Puerto/Servicio

```
nmap -T3 -Pn -f -sV 199.79.62.121 -oX nmap199.xml

Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-01 00:42 UTC
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.12s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      Pure-FTPd
22/tcp   open  ssh      OpenSSH 5.3 (protocol 2.0)
25/tcp   open  smtp     Exim smtpd 4.89
53/tcp   open  domain   ISC BIND 9.8.2rc1
80/tcp   open  http     Apache httpd 2.4.33 ((cPanel)
OpenSSL/1.0.2o mod_bwlimited/1.4 Phusion_Passenger/5.1.12)
110/tcp  open  pop3     Dovecot pop3d
143/tcp  open  imap     Dovecot imapd
443/tcp  open  ssl/http Apache httpd 2.4.33 ((cPanel)
OpenSSL/1.0.2o mod_bwlimited/1.4 Phusion_Passenger/5.1.12)
587/tcp  open  smtp     Exim smtpd 4.89
993/tcp  open  ssl/imap Dovecot imapd
995/tcp  open  ssl/pop3 Dovecot pop3d
3306/tcp open  mysql    MySQL 5.5.55-38.8-log
Service Info: OS: Red Hat Enterprise Linux 6; CPE:
cpe:/o:redhat:enterprise_linux:6

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.72 seconds
```

Fuente: Nmap 7.60.
Elaboración: Microsoft Office Word 2016.

Imagen 12: Escaneo sigiloso con Nmap para descubrimiento de sistema operativo

```
nmap -sS 199.79.62.121 -A
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-13 20:16 -05
Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing
Script Scan
NSE Timing: About 99.39% done; ETC: 20:17 (0:00:00 remaining)
Nmap scan report for 199.79.62.121
Host is up (0.13s latency).
Not shown: 984 filtered ports
PORT      STATE  SERVICE  VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp      Pure-FTPd
22/tcp    open   ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 be:2e:cf:cd:93:06:c2:41:4a:14:b8:ea:11:de:d5:f8 (DSA)
|_  2048 6b:ee:8b:3a:a3:04:e3:6a:74:d1:4c:50:76:e4:06:11 (RSA)
53/tcp    open   domain   ISC BIND 9.8.2rc1 (RedHat Enterprise
Linux 6)
| dns-nsid:
|_  bind.version: 9.8.2rc1-RedHat-9.8.2-0.62.rc1.el6_9.2
80/tcp    open   http     Apache httpd 2.4.33 ((cPanel)
OpenSSL/1.0.2o mod_bwlimited/1.4 Phusion_Passenger/5.1.12)
|_http-server-header: Apache/2.4.33 (cPanel) OpenSSL/1.0.2o
mod_bwlimited/1.4 Phusion_Passenger/5.1.12
|_http-title: Site doesn&apos;t have a title (text/html).
110/tcp   open   pop3     Dovecot pop3d
|_pop3-capabilities: TOP SASL(PLAIN LOGIN) USER STLS CAPA AUTH-
RESP-CODE PIPELINING UIDL RESP-CODES
|_ssl-date: 2018-07-14T01:17:41+00:00; 0s from scanner time.
143/tcp   open   imap     Dovecot imapd
|_imap-capabilities: STARTTLS more ID AUTH=PLAIN have ENABLE
capabilities Pre-login LITERAL+ IMAP4rev1 post-login
AUTH=LOGINA0001 listed SASL-IR NAMESPACE OK IDLE LOGIN-REFERRALS
```

```
| ssl-cert: Subject: commonName=cp-34.webhostbox.net
| Subject Alternative Name: DNS:cp-34.webhostbox.net,
DNS:www.cp-34.webhostbox.net
| Not valid before: 2018-05-12T00:00:00
|_Not valid after:  2019-05-12T23:59:59
|_ssl-date: 2018-07-14T01:17:40+00:00; 0s from scanner time.
443/tcp   open   ssl/http Apache httpd 2.4.33 ((cPanel)
OpenSSL/1.0.2o mod_bwlimited/1.4 Phusion_Passenger/5.1.12)
|_http-title: Site doesn&apos;t have a title (text/html).
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  h2
465/tcp   open   ssl/smtp Exim smtpd 4.89
| smtp-commands: cp-34.webhostbox.net Hello nmap.scanme.org
[179.7.192.21], SIZE 52428800, 8BITMIME, PIPELINING, AUTH PLAIN
LOGIN, HELP,
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP
QUIT RSET HELP
|_ssl-date: 2018-07-14T01:17:35+00:00; 0s from scanner time.
587/tcp   open   smtp     Exim smtpd 4.89
| smtp-commands: cp-34.webhostbox.net Hello nmap.scanme.org
[179.7.192.21], SIZE 52428800, 8BITMIME, PIPELINING, AUTH PLAIN
LOGIN, STARTTLS, HELP,
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA
BDAT NOOP QUIT RSET HELP
|_ssl-date: 2018-07-14T01:17:40+00:00; 0s from scanner time.
990/tcp   closed ftps
993/tcp   open   ssl/imap Dovecot imapd
|_imap-capabilities: listed more ID AUTH=PLAIN have ENABLE
capabilities Pre-login LITERAL+ IMAP4rev1 post-login
AUTH=LOGINA0001 SASL-IR NAMESPACE IDLE OK LOGIN-REFERRALS
```

```
|_ssl-date: 2018-07-14T01:17:34+00:00; +1s from scanner time.
995/tcp   open   ssl/pop3 Dovecot pop3d
|_pop3-capabilities: RESP-CODES TOP CAPA AUTH-RESP-CODE
SASL(PLAIN LOGIN) PIPELINING UIDL USER
| ssl-cert: Subject: commonName=cp-34.webhostbox.net
| Subject Alternative Name: DNS:cp-34.webhostbox.net,
DNS:www.cp-34.webhostbox.net
| Not valid before: 2018-05-12T00:00:00
|_Not valid after:  2019-05-12T23:59:59
|_ssl-date: 2018-07-14T01:17:33+00:00; +1s from scanner time.
3306/tcp  open   mysql    MySQL 5.5.55-38.8-log
| mysql-info:
|   Protocol: 10
|   Version: 5.5.55-38.8-log
|   Thread ID: 47591811
|   Capabilities flags: 65535
|   Some Capabilities: InteractiveClient,
SwitchToSSLAfterHandshake, LongPassword, LongColumnFlag,
SupportsCompression, Speaks41ProtocolOld, SupportsTransactions,
DontAllowDatabaseTableColumn, ODBCClient, Support41Auth,
Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis,
SupportsLoadDataLocal, FoundRows, IgnoreSigpipes,
ConnectWithDatabase, SupportsMultipleStatments,
SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: 15_bL6j3_cVcn~R[UvqX
|_  Auth Plugin Name: 88
8649/tcp  closed unknown
60020/tcp closed unknown
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10
(93%), Linux 2.6.39 (93%), Linux 3.4 (93%), WatchGuard Fireware
```

```
(93%), Linux 2.6.39 (93%), Linux 3.4 (93%), WatchGuard Fireware
11.8 (93%), Synology DiskStation Manager 5.1 (92%), Linux 3.10
(92%), Linux 3.1 - 3.2 (92%), Linux 2.6.32 - 2.6.39 (90%), Linux
2.6.32 - 3.0 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 22 hops
Service Info: Host: cp-34.webhostbox.net; OS: Linux; CPE:
cpe:/o:redhat:enterprise_linux:6

TRACEROUTE (using port 8649/tcp)
HOP RTT       ADDRESS
1   6.09 ms   192.168.0.1
2   ... 6
7   25.46 ms  10.95.156.38
8   30.92 ms  10.95.156.53
9   25.50 ms  10.95.156.54
10  21.44 ms  10.95.156.33
11  ...
12  19.24 ms  10.95.156.42
13  23.96 ms  10.95.156.61
14  ...
15  128.70 ms ae-4.r05.miamfl02.us.bb.gin.ntt.net (129.250.3.40)
16  108.46 ms ae-1.r21.miamfl02.us.bb.gin.ntt.net (129.250.4.88)
17  118.71 ms ae-4.r22.dllstx09.us.bb.gin.ntt.net
(129.250.2.219)
18  125.54 ms ae-2.r10.dllstx09.us.bb.gin.ntt.net (129.250.4.82)
19  ... 21
22  125.64 ms cp-34.webhostbox.net (199.79.62.121)

OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 101.14 seconds
```

Fuente: Nmap 7.60.
Elaboración: Microsoft Office Word 2016.

3. Obtener Acceso

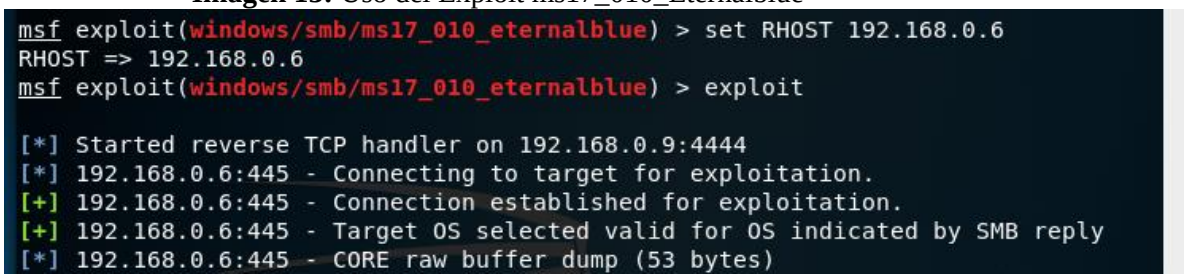
- Validación y explotación de las vulnerabilidades que hayan sido encontradas en el paso anterior.
- Escalamiento de privilegios.

Herramientas usadas:

- ✓ Metasploit.

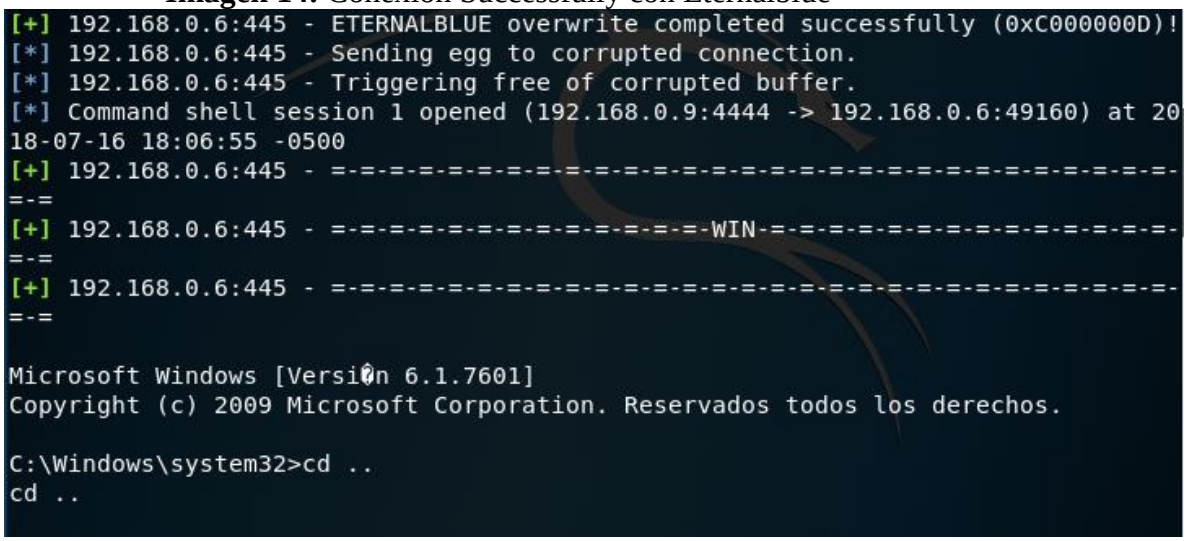
- Hacemos uso del exploit denominado eternalblue el cual es explotado usando Metasploit, obteniendo acceso a través de una Shell System por lo cual ya no sería necesario la obtención de permiso de administrador

Imagen 13: Uso del Exploit ms17_010_Eternalblue



Fuente: Metasploit.
Elaboración: Microsoft Office Word 2016.

Imagen 14: Conexión Successfully con Eternalblue



Fuente: Metasploit.
Elaboración: Microsoft Office Word 2016.

- En la Imagen N 13 se asigna la IP que será tacada con el comando “set RHOST”, en la Imagen 14 el exploit ya ha obtenido acceso a la maquina victima atreves de la Shell de system

4. Mantener Acceso

- Instalación de puertas traseras, troyanos, y elevación de privilegios.

5. Borrado de Huellas

- Se limpian los rastros para dificultar el trabajo del forense; se procede a deshabilitar Auditpol.exe

Anexo 15: Informe de Vulnerabilidades

INFORME DE VULNERABILIDADES ENCONTRADAS

ESCANEO DE PUERTOS VULNERABLES

TARGET: 199.79.62.121

Análisis de los Puertos Encontrados.

Tabla 9: Escaneo de todos los Puertos enocntrados

PUERTO	ESTADO	SERVICIO	PRODUCTO	VERSION	NIVEL DE RIESGO
21	Open	ftp	Pure-FTPd		INFO
22	Open	Ssh	OpenSSH	5.3	ALTO
25	Open	Smtp	Exim smtpd	4.89	ALTO
53	Open	Domain	ISC BIND	9.8.2rcl	INFO
80	Open	http	Apache httpd	2.4.33	INFO
110	Open	Pop3	Dovecot pop3d		INFO
143	Open	Ima	Dovecot imapd		INFO
443	Open	https	Apache https	2.4.33	INFO
465	Open	Smtp	Exim smtpd	4.89	ALTO
587	Open	Smtp	Exim smtpd	4.89	ALTO
993	Open	Imap	Dovecot imapd		INFO
995	Open	Pop3	Dovecot pop3d		INFO
3306	Open	mysql	MySQL	5.5.55-38.8-log	INFO

Fuente: OpenVas CE
Elaboración: Microsoft Office Word 2016.

Calificación de Riesgos	
Alto	4
Medio	0
Baja	0
Información	10

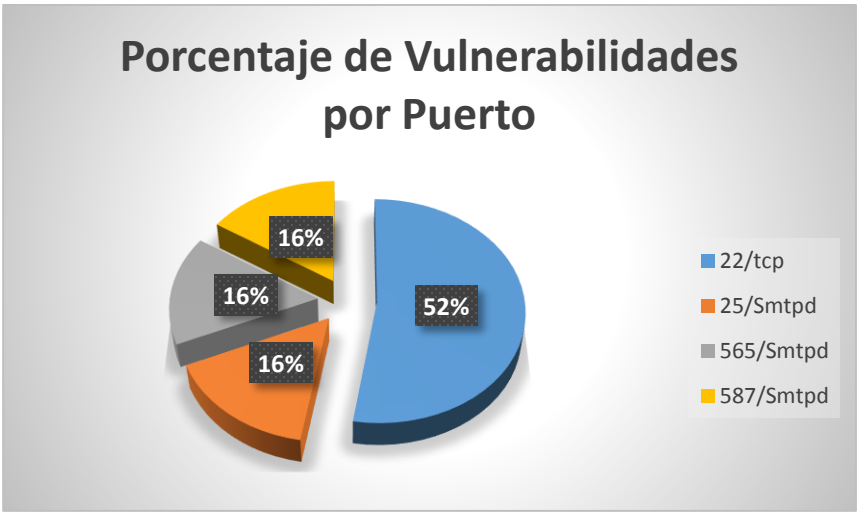
Fuente: OpenVas CE
Elaboración: Microsoft Office Word 2016.

- De los 13 puertos que fueron encontrados y luego escaneados se identificaron que cuatro puertos tenían al menos una vulnerabilidad con calificación de riesgo alto, que representan un 29% del total de vulnerabilidades como se aprecia en el siguiente gráfico.

Numero De Vulnerabilidades Por Puerto

Vulnerabilidades por Puerto	
22/tcp	10
25/Smtpd	3
565/Smtpd	3
587/Smtpd	3

- De los 13 puertos que fueron encontrados y luego escaneados se identificaron que el puerto 22 es el que presenta el mayor número de vulnerabilidades con un 52% del total luego con los mismos valores le siguen el puerto 25, 565, 587.

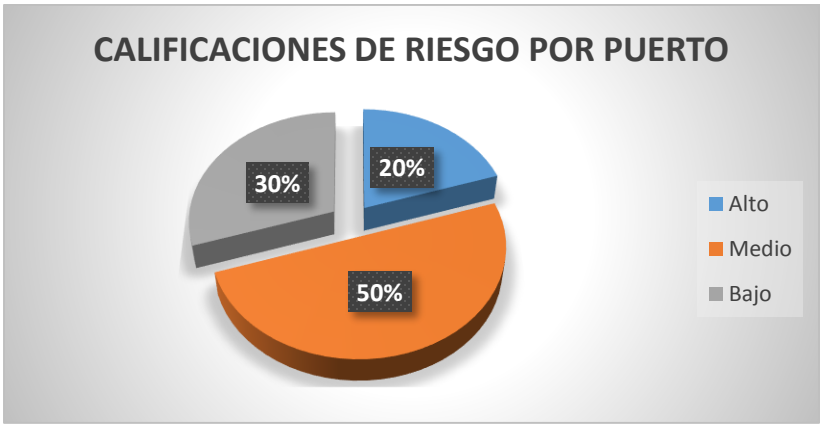


Fuente: OpenVas CE
Elaboración: Microsoft Office Word 2016.

Vulnerabilidades Encontradas para el Puerto 22

PUERTO 22/ssh	
Alto	2
Medio	5
Bajo	3

- En el Puerto 22 el cual presenta el mayor número de vulnerabilidades 2 de estas obtuvieron una calificación de riesgo alto siendo esta información importante a la hora de establecer que Honeypot brinda simula este servicio.



Vulnerabilities found for Openssh 5.3 (port 22/tcp)

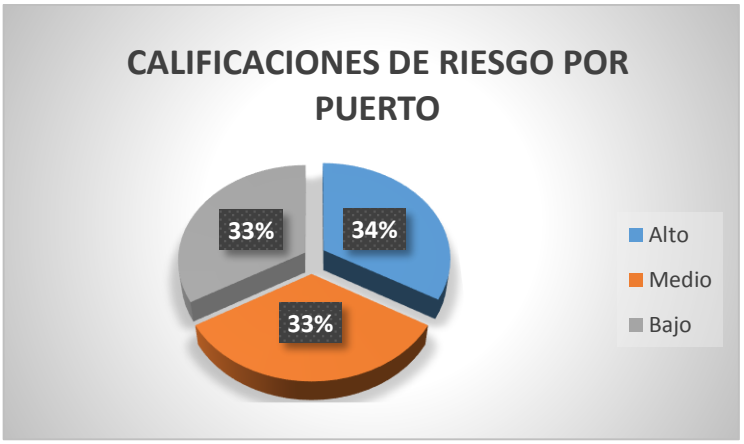
Risk level	CVSS	CVE	Summary	Exploit
	7.5	CVE-2014-1692	The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.	N/A
	7.5	CVE-2010-4478	OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.	N/A
	5.0	CVE-2016-10708	sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.	N/A
	5.0	CVE-2017-15906	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.	N/A
	5.0	CVE-2010-5107	The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.	N/A
	4.0	CVE-2016-0777	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.	EDB-ID:40962
	4	CVE-2010-4755	The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.	N/A
	3.5	CVE-2012-0814	The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.	N/A
	3.5	CVE-2011-5000	The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.	N/A
	2.1	CVE-2011-4327	ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.	N/A

canning/robot-attack-scanner

Vulnerabilidades Encontradas para el Puerto 25

PUERTO 25/Smtpd	
Alto	1
Medio	1
Bajo	1

- En el Puerto 25 presenta una total de 3 vulnerabilidades el cual presenta el 16% de del total de vulnerabilidades de las cuales se sitúa una vulnerabilidad para cada estado en la calificación de riesgo, Alto, Medio y Bajo.



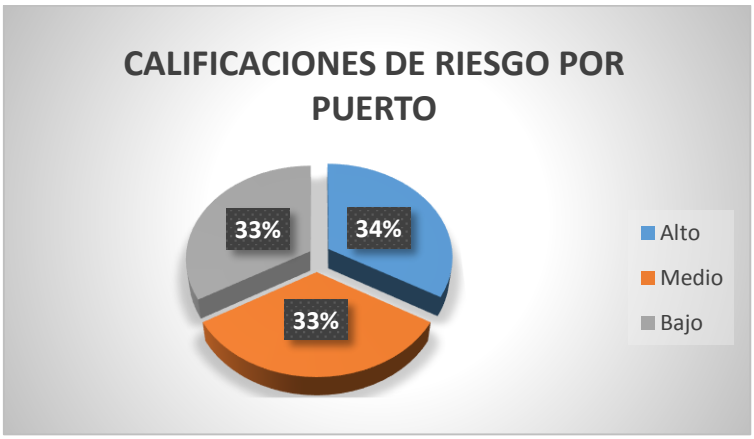
Vulnerabilities found for Exim Smtpd 4.89 (port 25/tcp)

Risk level	CVSS	CVE	Summary	Exploit
	7.5	CVE-2017-16943	The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands.	N/A
	5	CVE-2017-16944	The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to cause a denial of service (infinite loop and stack exhaustion) via vectors involving BDAT commands and an improper check for a '.' character signifying the end of the content, related to the bdat_getc function.	EDB-ID:43184
	2.1	CVE-2017-1000369	Exim supports the use of multiple "-p" command line arguments which are malloc()'ed and never free()'ed, used in conjunction with other issues allows attackers to cause arbitrary code execution. This affects exim version 4.89 and earlier. Please note that at this time upstream has released a patch (commit 65e061b76867a9ea7aeeb535341b790b90ae6c21), but it is not known if a new point release is available that addresses this issue at this time.	N/A

Vulnerabilidades Encontradas para el Puerto 465

PUERTO 465/Smtpd	
Alto	1
Medio	1
Bajo	1

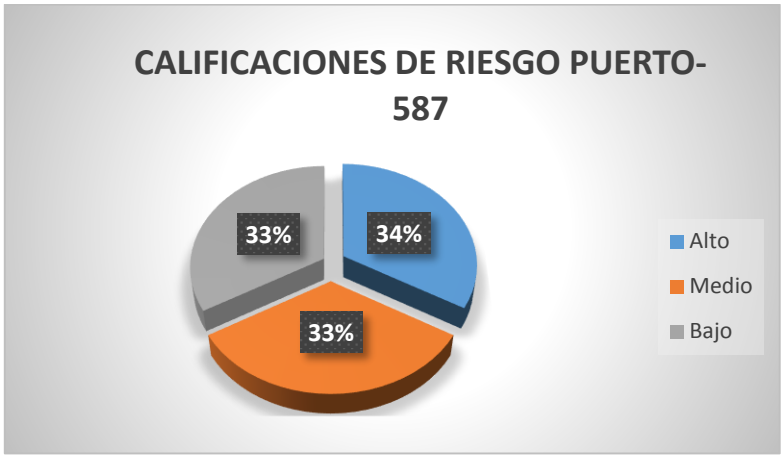
- En el Puerto 465 presenta una total de 3 vulnerabilidades el cual presenta el 16% de del total de vulnerabilidades de las cuales se sitúa una vulnerabilidad para cada estado en la calificación de riesgo, Alto, Medio y Bajo.



Vulnerabilities found for Exim Smtpd 4.89 (port 465/tcp)

Risk level	CVSS	CVE	Summary	Exploit
	7.5	CVE-2017-16943	The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands.	N/A
	5	CVE-2017-16944	The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to cause a denial of service (infinite loop and stack exhaustion) via vectors involving BDAT commands and an improper check for a '.' character signifying the end of the content, related to the bdat_getc function.	EDB-ID:43184
	2.1	CVE-2017-1000369	Exim supports the use of multiple "-p" command line arguments which are malloc()'ed and never free()'ed, used in conjunction with other issues allows attackers to cause arbitrary code execution. This affects exim version 4.89 and earlier. Please note that at this time upstream has released a patch (commit 65e061b76867a9ea7aeeb535341b790b90ae6c21), but it is not known if a new point release is available that addresses this issue at this time.	N/A

Vulnerabilidades Encontradas para el Puerto 587



- En el Puerto 587 presenta una total de 3 vulnerabilidades el cual presenta el 16% de del total de vulnerabilidades de las cuales se sitúa una vulnerabilidad para cada estado en la calificación de riesgo, Alto, Medio y Bajo.

Vulnerabilities found for Exim Smtpd 4.89 (port 587/tcp)

Risk level	CVSS	CVE	Summary	Exploit
	7.5	CVE-2017-16943	The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands.	N/A
	5	CVE-2017-16944	The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to cause a denial of service (infinite loop and stack exhaustion) via vectors involving BDAT commands and an improper check for a '.' character signifying the end of the content, related to the bdat_getc function.	EDB-ID:43184
	2.1	CVE-2017-1000369	Exim supports the use of multiple "-p" command line arguments which are malloc()'ed and never free()'ed, used in conjunction with other issues allows attackers to cause arbitrary code execution. This affects exim version 4.89 and earlier. Please note that at this time upstream has released a patch (commit 65e061b76867a9ea7aeeb5355341b790b90ae6c21), but it is not known if a new point release is available that addresses this issue at this time.	N/A

Anexo 16: Calificación de riesgo de las alertas encontradas

Escaneo del sitio web con owasp

Calificación de Riesgos	Numero de Alertas
Alto	0
Medio	1
Bajo	3
Información	0

Fuente: OWASP 7.0
Elaboración: Microsoft Office Word 2016

Medio (Medio)	X-Frame-Options Header Not Set
Descripción	El encabezado X-Frame-Options no está incluido en la respuesta HTTP para proteger contra los ataques de 'ClickJacking'.
URL	http://munivictorlarco.gob.pe/
Método	GET
Parámetro	X-Frame-Options
Instancia	1
Solución	La mayoría de los navegadores web modernos admiten el encabezado HTTP X-Frame-Options. Asegúrese de que esté configurado en todas las páginas web devueltas por su sitio (si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET), entonces querrá usar SAMEORIGIN; de lo contrario, nunca esperará que la página para enmarcar debe usar DENY. ALLOW-FROM permite que sitios web específicos marquen la página web en navegadores web compatibles).
Referencia	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	X-Content-Type-Options Header Missing
Descripción	El encabezado Anti-MIME-X-Content-Type-Options no se configuró en 'nosniff'. Esto permite a las versiones anteriores de Internet Explorer y Chrome realizar el rastreo de MIME en el cuerpo de la respuesta, lo que puede causar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si está configurado), en lugar de realizar el rastreo de MIME.
URL	http://munivictorlarco.gob.pe/images/wp11.jpg http://munivictorlarco.gob.pe/images/logo.png http://munivictorlarco.gob.pe/images/wp9.jpg http://munivictorlarco.gob.pe/images/01.gif http://munivictorlarco.gob.pe/images/wp3.jpg http://munivictorlarco.gob.pe/jquery/core.js http://munivictorlarco.gob.pe/jquery/imagebox.js

URL	http://munivictorlarco.gob.pe/jquery/event.js http://munivictorlarco.gob.pe/jquery/carousel.js http://munivictorlarco.gob.pe/Scripts/AC_RunActiveContent.js http://munivictorlarco.gob.pe/jquery/isortables.js http://munivictorlarco.gob.pe/jquery/iselect.js http://munivictorlarco.gob.pe/images/07.gif http://munivictorlarco.gob.pe/jquery/fx.js http://munivictorlarco.gob.pe/images/wp10.jpg http://munivictorlarco.gob.pe/jquery/islideshow.js http://munivictorlarco.gob.pe/jquery/ittabs.js http://munivictorlarco.gob.pe/images/wp5.jpg
Método	GET
Parámetro	X-Content-Type-Options.
Instancia	46
Solución	Asegúrese de que la aplicación / servidor web configure el encabezado de tipo de contenido de manera adecuada y que establezca el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese de que el usuario final utilice un navegador web moderno y compatible con los estándares que no realice ningún tipo de detección MIME, o que la aplicación web / servidor web pueda indicarle que no realice el rastreo MIME.
Otra Información	Este problema aún se aplica a las páginas de tipo de error (401, 403, 500, etc.) ya que esas páginas a menudo aún se ven afectadas por problemas de inyección, en cuyo caso los navegadores siguen preocupados por olfatear páginas de su tipo de contenido real. En el umbral "Alto", este escáner no alertará sobre las respuestas de error del cliente o del servidor.
Referencia	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

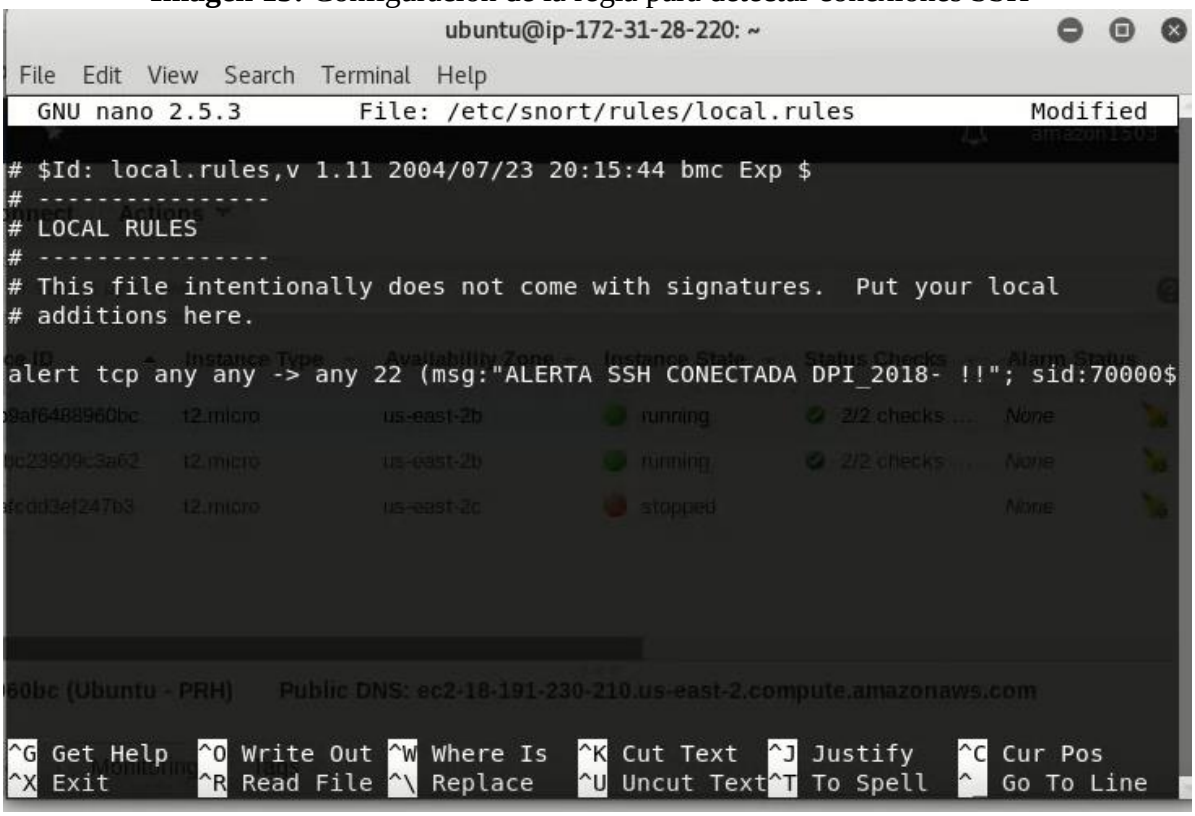
Low (Medium)	**Cross-Domain JavaScript Source File Inclusión**
Descripción	La página incluye uno o más archivos de script de un dominio de terceros.
URL	http://munivictorlarco.gob.pe/
Método	GET
Parámetro	http://stats.byspirit.ro/track.js

Evidencia	<script language="JavaScript" src="http://stats.byspirit.ro/track.js" type="text/javascript"></script>
Instancia	1
Solución	Asegúrese de que los archivos fuente de JavaScript se carguen solo de fuentes confiables y que los orígenes de los datos no puedan ser controlados por los usuarios finales de la aplicación.
Referencia	No encontrada
CWE Id	829
WASC Id	15
Source ID	3

Low (Medium)	**Navegador web Protección XSS no habilitada**
Descripción	Navegador web La protección XSS no está habilitada, o está desactivada por la configuración del encabezado de respuesta HTTP 'X-XSS-Protection' en el servidor web
URL	http://munivictorlarco.gob.pe/sitemap.xml
Método	GET
Parámetro	X-XSS-Protection
Instancia	1
Solución	Asegúrese de que el filtro XSS del navegador web esté habilitado, configurando el encabezado de respuesta HTTP de X-XSS-Protection en '1'.
Otra Información	El encabezado de respuesta HTTP de protección X-XSS permite que el servidor web habilite o deshabilite el mecanismo de protección XSS del navegador web. Los siguientes valores intentarían habilitarlo: X-XSS-Protection: 1; modo = bloque X-XSS-Protection: 1; informe = http: //www.example.com/xss Los siguientes valores lo deshabilitarían: X-XSS-Protection: 0 El encabezado de respuesta HTTP X-XSS-Protection actualmente es compatible con Internet Explorer, Chrome y Safari (WebKit). Tenga en cuenta que esta alerta solo se genera si el cuerpo de la respuesta podría contener una carga útil XSS (con un tipo de contenido basado en texto, con una longitud distinta de cero).
Referencia	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

Anexo 17: Configuración Snort

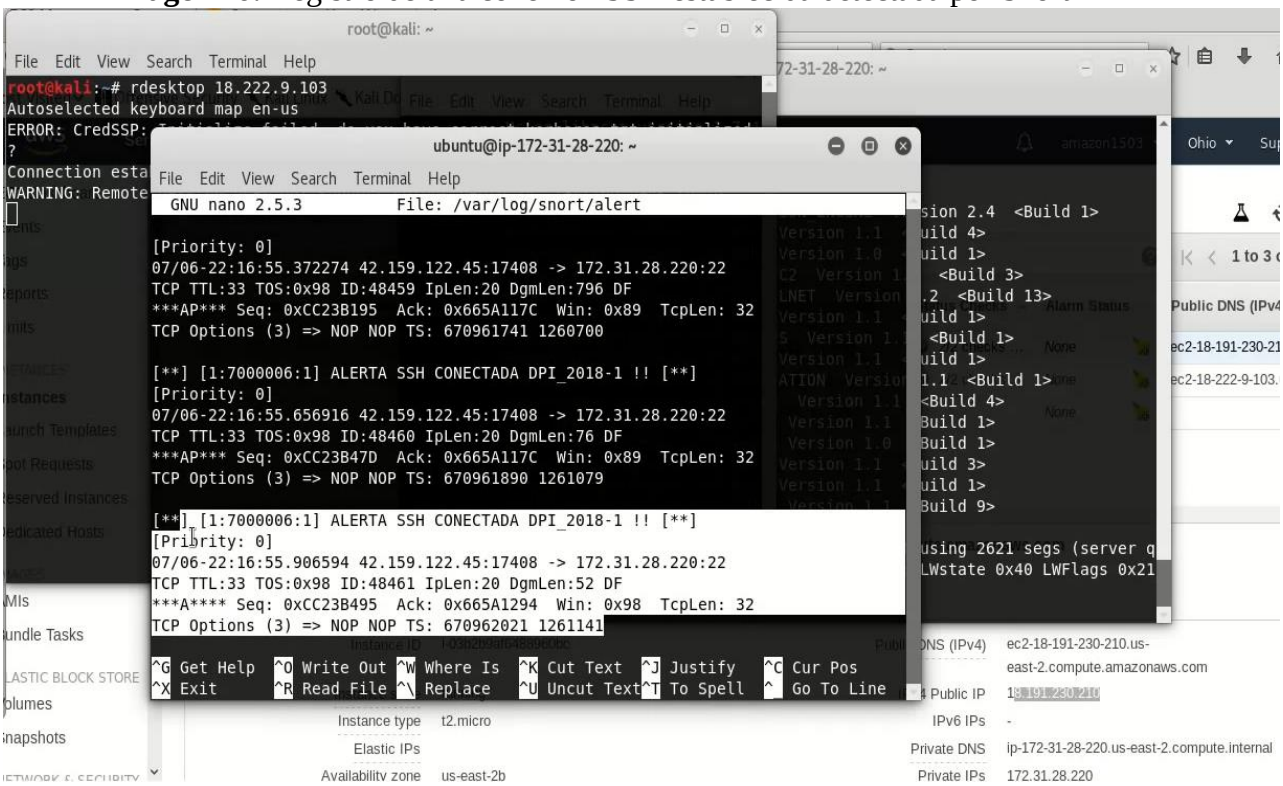
Imagen 15: Configuración de la regla para detectar conexiones SSH



Fuente: Snort.
Elaboración: Microsoft Office Word 2016

- En la última línea se establece como regla local que todas las conexiones que tengan como destino el puerto 22 genere un mensaje de alerta en el archivo log de Snort

Imagen 16: Registro de una conexión SSH establecida detectada por Snort



Fuente: Snort.
Elaboración: Microsoft Office Word 2016.

- En el texto seleccionado que pertenece al archivo Log de Snort se puede identificar el mensaje de alerta donde indica que se ha establecido una conexión SSH y muestra desde que dirección IP se realizo

Anexo 18: Configuración de Kippo

Imagen17: Configuración de Kippo

```
[honeypot]
ssh_port = 22
hostname = PROServer
log_path = log
download_path = dl
contents_path = honeyfs
filesystem_file = fs.pickle
data_path = data
txtcmds_path = txtcmds
rsa_public_key = data/ssh_host_rsa_key.pub
rsa_private_key = data/ssh_host_rsa_key
dsa_public_key = data/ssh_host_dsa_key.pub
dsa_private_key = data/ssh_host_dsa_key
exec_enabled = true
fake_addr = 192.168.0.5
ssh_version_string = OpenSSH 5.3 (protocol 2.0)
interact_enabled = true
interact_port = 5000
```

Fuente: Archivo de configuración de Kippo
Elaboración: Microsoft Office Word 2016

- En la imagen podemos observar la configuración que presenta el Honeypot, se establece el servicio SSH en el puerto 22 también se asignan el directorio donde se guardarán el registro de información obtenida por alguna intrusión, se asigna la dirección IP falsa, así como la versión del SSH tal cual como nos saliera en un escaneo con Nmap, (ver imagen 12)

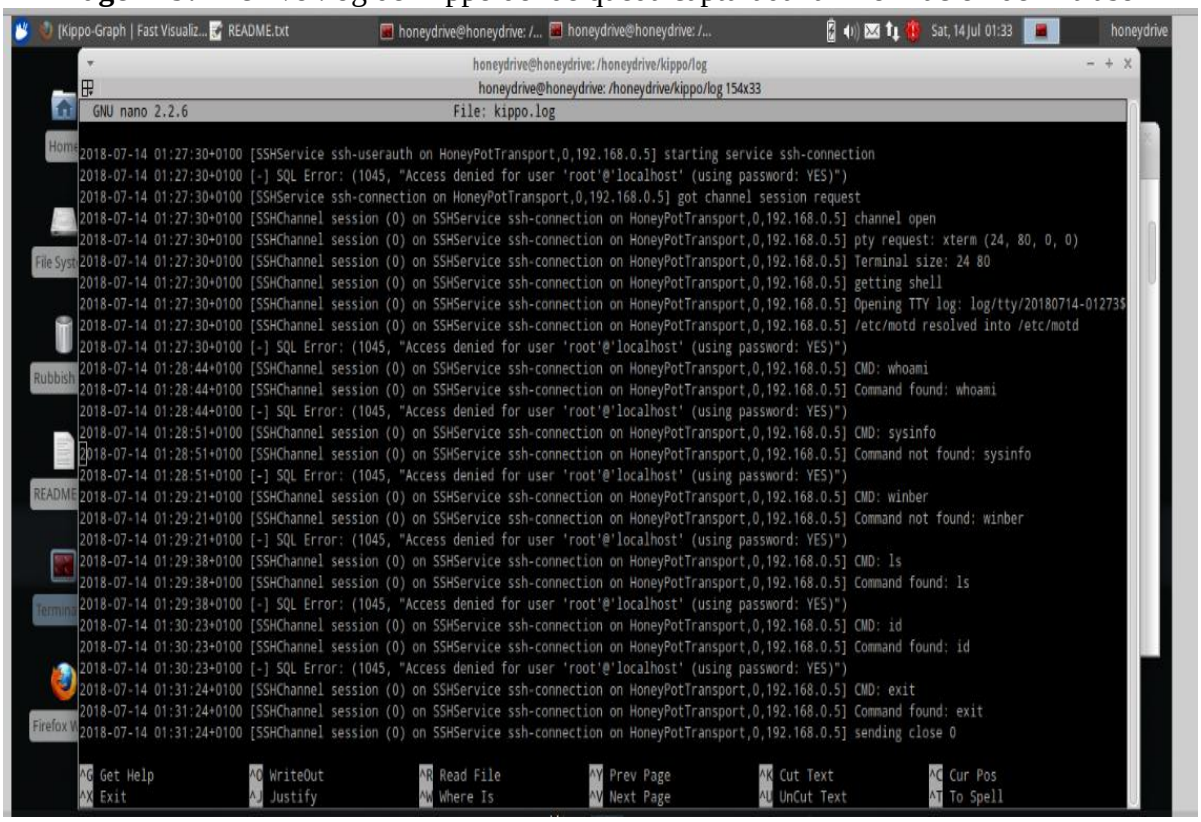
Imagen 18: Archivo Log donde se registran las intrusiones

```
2018-07-10 02:44:55+0100 [-] Log opened.
2018-07-10 02:44:55+0100 [-] twistd 11.1.0 (/usr/bin/python 2.7.3) starting up.
2018-07-10 02:44:55+0100 [-] reactor class: twisted.internet.pollreactor.PollReactor.
2018-07-10 02:44:55+0100 [-] HoneyPotSSHFactory starting on 22
2018-07-10 02:44:55+0100 [-] Starting factory <kippo.core.honeypot.HoneyPotSSHFactory instance at 0x977690c>
2018-07-10 03:32:57+0100 [kippo.core.honeypot.HoneyPotSSHFactory] New connection: 192.168.0.4:56609 (192.168.0.5:22) [session: 0]
2018-07-10 03:32:57+0100 [HoneyPotTransport,0,192.168.0.4] Remote SSH version: SSH-2.0-PuTTY_Release_0.70
2018-07-10 03:32:57+0100 [HoneyPotTransport,0,192.168.0.4] kex alg, key alg: diffie-hellman-group1-sha1 ssh-rsa
2018-07-10 03:32:57+0100 [HoneyPotTransport,0,192.168.0.4] outgoing: aes256-ctr hmac-sha1 none
2018-07-10 03:32:57+0100 [HoneyPotTransport,0,192.168.0.4] incoming: aes256-ctr hmac-sha1 none
```

Fuente: Archivo. Log de Kippo
Elaboración: Microsoft Office Word 2016

- En esta captura de una parte del archive log de Kippo se puede identificar que se abierto una conexión SSH con el uso de la herramienta PuTTY, tenemos la IP de origen de la conexión

Imagen 19: Archivo .log de Kippo donde queda capturada la información del intruso



Fuente: Archivo. Log de Kippo
Elaboración: Microsoft Office Word 2016

- En esta imagen podemos revisar la actividad realizada por el intruso y se obtiene una lista de los comandos ingresados por este, se puede concluir que el intruso está realizando una exploración de archive con el comando "ls" o "sysinfo" para obtener información más a detalle del servidor en este caso

Anexo 19: Presupuesto

Tabla 10: Presupuesto

GASTOS	DESCRIPCIÓN	CANT	PRECIO POR	COSTO TOTAL
A	**PERSONAL**			
1	Tesista	1	0.00	0.00
2	Asesor	1	0.00	0.00
3	Docente	1	0.00	0.00
Sub Total S/.				**S/. 0.00**
B	**MATERIALES**			
1	Lapicero Pilot	12	1.00	12.00
2	Papel Bond A4	01	0.025	25.00
3	Memoria USB KINGSTON 32GB	01	0.00	60.00
4	Memoria USB KINGSTON 16GB	01	0.00	45.00
5	Memoria USB KINGSTON 8GB	01		35.00
6	Fólder manila	12	0.50	6.00
7	CD's – R700MB	09	1.00	9.00
8	CD's – R4GB	04	2.00	8.00
Sub Total S/.				**S/. 200.00**
C	**SERVICIOS**			
1	Internet	8	120.00	480.00
2	Movilidad	60	4.00	240.00
3	Fotocopiado	100	0.05	10.00
4	Impresiones	1500	0.20	300.00
5	Servicio de luz	4	80.00	320.00
Sub Total S/.				**1350.00 S/**
Total, S/.				**1550.00 S/**

Tabla 11: Flujo de Caja

AÑEXOS / INGRESOS	Año 0		Año 1	Año 2	Año 3	Año 4
	0.00		**3,586.13**	**3,699.19**	**3,778.34**	**3812.26**
Ahorro en Horas de Trabajo			3,360.00	3,360.00	3,360.00	3360.00
Ingresos Proyectados			226.13	339.19	418.34	452.26
EGRESOS	**1,550.00**		**2,000.01**	**2,000.01**	**2,000.01**	**2000.01**
Costo de Inversión y Desarrollo	1,550.00					
Software	00.00					
Materiales	200.00					
Hardware	32.70					
Personal	460.00					
Servicios	1,350.00					
Costos de Operación			**2,000.01**	**2,000.01**	**2,000.01**	**2,000.01**
Inflación Aproximada (8%)			160.00	160.00	160.00	160.00
Flujo de Caja del Proyecto	**-1,550.00**		**1,586.12**	**1,698.99**	**1,778.33**	**1812.26**
Acumulado	**-1,550.00**		**36.12**	**3,361.86**	**5,140.19**	**6,952.45**

Fuente: Costos y Presupuestos (Anexo N° XII)
Elaboración: Microsoft Office Word 2016.

En la caja de flujo presentada se detallan los costos de inversión (Tabla N° 5), se describe el detalle de los costos de Inversión, desarrollo y operacionales que son los Egresos, a su vez los montos en cuanto a los Ingresos, a su vez el Flujo de Caja proyectado a 4 años.

Análisis de Rentabilidad

A. Valor Actual Neto (VAN)

Tasa (TMAR)= 15% - Fuente: Banco de Crédito del Perú.

$$\mathbf{VAN} = -1550.00 + \frac{(3586.13 - 2000.00)}{(1+0.15)} + \frac{(3699.13 - 2000.00)}{(1+0.15)^2} + \frac{(3778.34 - 2000.00)}{(1+0.15)^3}$$

$$\mathbf{VAN} = 3331.91$$

Interpretación: El valor actual que genera el proyecto es de S/. 3331.91. El VAN mayor a cero, conviene ejecutar el proyecto.

A. Relación Beneficio/Costo (B/C)

Formula:

$$\frac{\mathbf{B}}{\mathbf{C}} = \frac{\text{VAB}}{\text{VAC}} \cdots$$

- **VAB** = Inversión inicial o flujo caja en el periodo 0.

$$\mathbf{VAB} = -1550\frac{3586.13}{1+0.15} + \frac{3699.19}{(1+0.15)^2} + \frac{3778.34}{(1+0.15)^3} + \frac{3812.26}{(1+0.15)^4}$$

VAB = 10584.96

- **VAC** = Total de beneficios tangibles.

$$\mathbf{VAC} = 1550 + \frac{2000.00}{(1+0.15)} + \frac{2000.00}{(1+0.15)^2} + \frac{2000.00}{(1+0.15)^3}$$

VAC = 7262.93

Reemplazamos los valores de VAB y VAC en la fórmula:

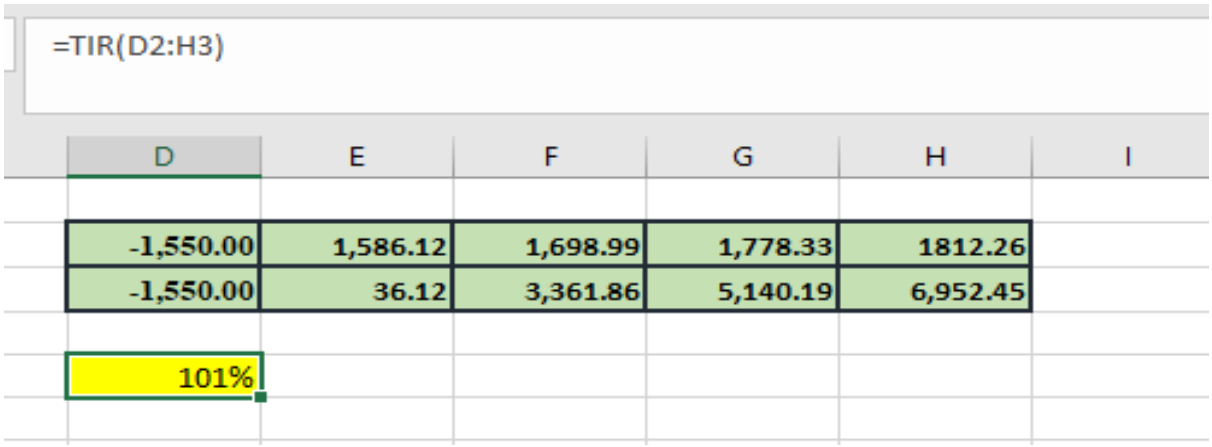
$$\mathbf{B/C} = \frac{17209.01}{10584.96}$$

$$\frac{\mathbf{B}}{\mathbf{C}} = 1.45$$

Interpretación: Por cada Nuevo sol que se invierte, obtendremos una ganancia de S/. 0.45.

B. TIR (Tasa interna de retorno):

$$0 = -\text{lo} + \frac{B-C}{(1+0.16)} + \frac{B-C}{(1+0.16)^2} + \frac{B-C}{(1+0.16)^3}$$



TIR = 101%

C. Tiempo de Recuperación de Capital:

$$\mathbf{TR} = \frac{1550.00}{3586.13 - 2000.00}$$

$$\mathbf{TR} = \frac{1550.00}{1586.13}$$

$$\mathbf{TR} = 0.97$$

Para determinar los meses y días se hará la respectiva conversión

$$0{,}97 * \frac{12\ meses}{1\ año} = 11.94 \approx 11 \text{ meses}$$

$$0{,}64 * \frac{30\ días}{1\ mes} = 19.2 \approx 19 \text{ días}$$

Tiempo de Recuperación de Capital será en 0 año, 11 meses y 19 días.

- **Conclusiones de la Evaluación Económica**

VAN = 3331.91 > 0
B/C = 1.45 > 1
TIR = 101%

Como conclusión, la Municipalidad Distrital de Víctor Larco Herrera obtiene beneficios al invertir en este proyecto.