UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS DE LAS VULNERABILIDADES DE LA RED DE DATOS DE LA EMPRESA PYME “MARCELO RÚALES” DE LA CIUDAD DE GUAYAQUIL, UTILIZANDO LA HERRAMIENTA POISONTAP PARA EL HACKING ÉTICO E INYECCIÓN DE PUERTAS TRASERAS Y CAPTURA DE TRAFICO HTTP-HTTPS, INCORPORANDO LAS RECOMENDACIONES NECESARIAS PARA SU MITIGACIÓN.

PROYECTO DE TITULACIÓN

Previa a la obtención del Título de:

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

AUTORES:

MARIO DANILO JALCA MANZABA

DIANA SHIRLEY CUJI TOALOMBO

TUTOR:

ING. FRANCISCO ÁLVAREZ Mgs.

GUAYAQUIL – ECUADOR

2018

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE GRADUACIÓN

TÍTULO:	ANÁLISIS DE LAS VULNERABILIDADES DE LA RED DE DATOS DE LA EMPRESA PYME "MARCELO RÚALES" DE LA CIUDAD DE GUAYAQUIL, UTILIZANDO LA HERRAMIENTA POISONTAP PARA EL HACKING ÉTICO E INYECCIÓN DE PUERTAS TRASERAS Y CAPTURA DE TRAFICO HTTP-HTTPS, INCORPORANDO LAS RECOMENDACIONES NECESARIAS PARA SU MITIGACIÓN.
AUTOR(ES)(apellidos/nombres):	MARIO DANILO JALCA MANZABA DIANA SHIRLEY CUJI TOALOMBO
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):	Ing. ING. FRANCISCO ÁLVAREZ Mgs.
INSTITUCIÓN:	Universidad Estatal de Guayaquil
FACULTAD:	Ciencias Matemáticas y Físicas
CARRERA:	Ingeniería en Networking y Telecomunicaciones
GRADO OBTENIDO:	Ingeniero en Networking y Telecomunicaciones
FECHA DE PUBLICACIÓN:	**No. DE PÁGINAS:**
ÁREAS TEMÁTICAS:	
PALABRAS CLAVES /KEYWORDS:	

RESUMEN/ABSTRACT (150-250 palabras): En este presente proyecto de titulación se identificó la problemática actual que presentan las tecnologías de la información implementada en las empresas, además en el marco teórico se detalló el funcionamiento del miniordenador Raspberry PI Zero en donde este es participe fundamental de la propuesta tecnológica, también se realizaron las respectivas pruebas de conexión con los dispositivos periféricos, descarga e instalación de NOOBS, configuración de los paquetes POISONTAP y del archivo INSTALL.SH, también se determinó que el ataque que efectúa POISONTAP es netamente pasivo ya que cumple con la funcionalidad de capturar tráfico generado por un computador cliente, una vez conectada la placa electrónica con la estación de trabajo emula una interfaz ETHERNET por medio del puerto USB (Universal Serial Bus).

ADJUNTO PDF:		**SI**		**NO**
CONTACTO CON AUTOR/ES:	**Teléfono**: 0968090525		**E-Mail**: diana.cujit@ug.edu.ec	
	Teléfono: 0978748377		**E-Mail**: mario.jalcam@ug.edu.ec	
CONTACTO CON LA INSTITUCIÓN:	**Nombre**:			
	Teléfono:			
	E-Mail:			

CARTA DE APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de titulación, **"**ANÁLISIS DE LAS VULNERABILIDADES DE LA RED DE DATOS DE LA EMPRESA PYME "MARCELO RÚALES" DE LA CIUDAD DE GUAYAQUIL, UTILIZANDO LA HERRAMIENTA POISONTAP PARA EL HACKING ÉTICO E INYECCIÓN DE PUERTAS TRASERAS Y CAPTURA DE TRAFICO HTTP-HTTPS, INCORPORANDO LAS RECOMENDACIONES NECESARIAS PARA SU MITIGACIÓN.**"**, elaborado por el **Sres.: JALCA MANZABA MARIO DANILO** y **CUJI TOALOMBO DIANA SHIRLEY**, alumno no titulado de la Carrera de Ingeniería en Networking y Telecomunicaciones de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Networking y Telecomunicaciones, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

Atentamente,

_____

ING. FRANCISCO ÁLVAREZ Mgs.

TUTOR

DEDICATORIA

Dedico este proyecto a mis padres que me supieron apoyar en todo momento, a mi tío que me brindo sus consejos de vida y a mi pareja incondicional que ha estado pendiente de mis logros y ha sido participe fundamental de cada uno de ellos y a los docentes que me supieron encaminar a ser mejor en todo ámbito para alcanzar esta meta de ser Ingeniero.

JALCA MANZABA MARIO DANILO

DEDICATORIA

A mi familia por darme su apoyo incondicional, por ser mi pilar fundamental, a los docentes que supieron brindarme su ayuda en asesoría y con el conocimiento para mi formación profesional.

CUJI TOALOMBO DIANA SHIRLEY

AGRADECIMIENTO

Agradezco a Dios, mis padres, mis hermanos, familiares y en especial a mi esposa por todo el apoyo que me han brindado durante estos años, por ellos y para ellos es mi Título.

JALCA MANZABA MARIO DANILO

AGRADECIMIENTO

Agradezco a Dios por haberme concedido salud y la fuerza necesaria para superar cada obstáculo.

A mis padres, hermanos y todos aquellos que me han ayudado a cumplir esta meta de ser ingeniero.

CUJI TOALOMBO DIANA SHIRLEY

TRIBUNAL PROYECTO DE TITULACIÓN

Ing. Eduardo Santos Baquerizo, M.Sc.

DECANO DE LA FACULTAD CC.MM.FF

Ing. Harry Luna Aveiga, M.Sc.

DIRECTOR

CINT

Ing. Francisco Álvarez, Mgs.

PROFESOR DIRECTOR DEL PROYECTO DE TITULACIÓN

Ing. Jacobo Ramirez, Mgs.

PROFESOR TUTOR REVISOR DEL PROYECTO DE TITULACIÓN

Ab. Juan Chávez A.

SECRETARIO

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Proyecto de Titulación, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la UNIVERSIDAD DE GUAYAQUIL"

JALCA MANZABA MARIO DANILO

CUJI TOALOMBO DIANA SHIRLEY

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS DE LAS VULNERABILIDADES DE LA RED DE DATOS DE LA EMPRESA PYME “MARCELO RÚALES” DE LA CIUDAD DE GUAYAQUIL, UTILIZANDO LA HERRAMIENTA POISONTAP PARA EL HACKING ÉTICO E INYECCIÓN DE PUERTAS TRASERAS Y CAPTURA DE TRAFICO HTTP-HTTPS, INCORPORANDO LAS RECOMENDACIONES NECESARIAS PARA SU MITIGACIÓN.

Proyecto de Titulación que se presenta como requisito para optar por el título de

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

Autores: MARIO DANILO JALCA MANZABA

C.I. 0925676942

DIANA SHIRLEY CUJI TOALOMBO

C.I. 0927354597

Tutor: Ing. FRANCISCO ÁLVAREZ Mgs.

Guayaquil, septiembre de 2018

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del proyecto de titulación, nombrado por el Consejo Directivo de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil.

CERTIFICO:

Que he analizado el Proyecto de Titulación presentado por los estudiantes MARIO DANILO JALCA MANZABA, DIANA SHIRLEY CUJI TOALOMBO, como requisito previo para optar por el título de Ingeniero en Networking y Telecomunicaciones cuyo tema es:

ANÁLISIS DE LAS VULNERABILIDADES DE LA RED DE DATOS DE LA EMPRESA PYME “MARCELO RÚALES” DE LA CIUDAD DE GUAYAQUIL, UTILIZANDO LA HERRAMIENTA POISONTAP PARA EL HACKING ÉTICO E INYECCIÓN DE PUERTAS TRASERAS Y CAPTURA DE TRAFICO HTTP-HTTPS, INCORPORANDO LAS RECOMENDACIONES NECESARIAS PARA SU MITIGACIÓN.

Considero aprobado el trabajo en su totalidad.

Presentado por:

MARIO DANILO JALCA MANZABA	C.I. 0925676942
DIANA SHIRLEY CUJI TOALOMBO	C.I. 0927354597

Tutor: Ing. FRANCISCO ÁLVAREZ Mgs.

Guayaquil, septiembre de 2018

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

Autorización para Publicación de Proyecto de Titulación en Formato Digital

1. Identificación del Proyecto de Titulación

Nombre Alumno: Mario Danilo Jalca Manzaba	
Dirección: Coop. Santa Martha I Mz. 5 Solar 14	
Teléfono: 0978748377	**E-mail:** mario.jalcam@ug.edu.ec

Nombre Alumno: Diana Shirley Cují Toalombo	
Dirección: Isla Trinitaria I Coop. Luchar y Vencer Mz. M Solar 12	
Teléfono: 0968090525	**E-mail:** diana.cujit@ug.edu.ec

Facultad: Ciencias Matemáticas y Físicas
Carrera: Ingeniería en Networking y Telecomunicaciones
Título al que opta: Ingeniero en Networking y Telecomunicaciones
Profesor Guía: Ing. Francisco Álvarez Mgs.

Título del Proyecto de Titulación: ANÁLISIS DE LAS VULNERABILIDADES DE LA RED DE DATOS DE LA EMPRESA PYME “MARCELO RÚALES” DE LA CIUDAD DE GUAYAQUIL, UTILIZANDO LA HERRAMIENTA POISONTAP PARA EL HACKING ÉTICO E INYECCIÓN DE PUERTAS TRASERAS Y CAPTURA DE TRAFICO HTTP-HTTPS, INCORPORANDO LAS RECOMENDACIONES NECESARIAS PARA SU MITIGACIÓN.

Tema del Proyecto de Titulación: ANÁLISIS DE LAS VULNERABILIDADES DE LA RED DE DATOS DE LA EMPRESA PYME “MARCELO RÚALES” DE LA CIUDAD DE GUAYAQUIL, UTILIZANDO LA HERRAMIENTA POISONTAP PARA EL HACKING ÉTICO E INYECCIÓN DE PUERTAS TRASERAS Y CAPTURA DE TRAFICO HTTP-HTTPS, INCORPORANDO LAS RECOMENDACIONES NECESARIAS PARA SU MITIGACIÓN.

2. Autorización de Publicación de Versión Electrónica del Proyecto de Titulación

A través de este medio autorizo a la Biblioteca de la Universidad de Guayaquil y a la Facultad de Ciencias Matemáticas y Físicas a publicar la versión electrónica de este Proyecto de titulación.

Publicación electrónica:

Inmediata		Después de 1 año	

Firma Alumno:

3. Forma de envío:

El texto del proyecto de titulación debe ser enviado en formato Word, como archivo .Doc. O .RTF y. Puf para PC. Las imágenes que la acompañen pueden ser: .gif, .jpg o .TIFF.

	DVDROM	CDROM	

ÍNDICE GENERAL

ABREVIATURAS

UG	Universidad de Guayaquil
CC.MM.FF	Facultad de Ciencias Matemáticas y Física
ISO	Organización de Estándares Internacionales
HTTP	Protocolo de Transferencia de Hipertexto
HTTPS	Protocolo de Transferencia de Hipertexto en modo seguro
PT	Poisontap

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANÁLISIS DE LAS VULNERABILIDADES DE LA RED DE DATOS DE LA EMPRESA PYME "MARCELO RÚALES" DE LA CIUDAD DE GUAYAQUIL, UTILIZANDO LA HERRAMIENTA POISONTAP PARA EL HACKING ÉTICO E INYECCIÓN DE PUERTAS TRASERAS Y CAPTURA DE TRAFICO HTTP-HTTPS, INCORPORANDO LAS RECOMENDACIONES NECESARIAS PARA SU MITIGACIÓN.

Autores: MARIO DANILO JALCA MANZABA

DIANA SHIRLEY CUJI TOALOMBO

Tutor: Ing. FRANCISCO ÁLVAREZ Mgs.

RESUMEN

En este presente proyecto de titulación se identificó la problemática actual que presentan las tecnologías de la información implementada en las empresas, además en el marco teórico se detalló el funcionamiento del miniordenador Raspberry PI Zero en donde este es participe fundamental de la propuesta tecnológica, también se realizaron las respectivas pruebas de conexión con los dispositivos periféricos, descarga e instalación de NOOBS, configuración de los paquetes PT y del archivo INSTALL.SH, también se determinó que el ataque que efectúa PT es netamente pasivo ya que cumple con la funcionalidad de capturar tráfico generado por un computador cliente, una vez conectada la placa electrónica con la estación de trabajo emula una interfaz ETHERNET por medio del puerto USB (Universal Serial Bus).

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ANALYSIS OF THE VULNERABILITIES OF THE DATA NETWORK OF THE SMALL BUSINESS "MARCELO RÚALES" OF THE CITY OF GUAYAQUIL, USING THE POISONTAP TOOL FOR ETHICAL HACKING AND INJECTION OF REAR DOORS AND HTTP-HTTPS TRAFFIC CAPTURE, INCORPORATING THE RECOMMENDATIONS NECESSARY FOR MITIGATION.

Authors: MARIO DANILO JALCA MANZABA

DIANA SHIRLEY CUJI TOALOMBO

Advisor: Ing. FRANCISCO ÁLVAREZ Mgs.

ABSTRACT

In this present project of titillation identified the problematic current that present the technologies of the information implemented in the companies, in addition in the theoretical frame detail the operation of the minicomputer Raspberry PI Zero where this is fundamental participant of the technological proposal, also they made the respective tests of connection with the peripheral devices, download and installation of NOOBS, configuration of the PT packages and the file INSTALL.SH, it was also determined that the attack made by PT is clearly passive since it fulfills the functionality of capturing traffic generated by a client computer, once the electronic board is connected to the workstation it emulates an ETHERNET interface through the USB (Universal Serial Bus) port.

INTRODUCCIÓN

Actualmente los profesionales de seguridad informática utilizan sistemas operativos Linux y componentes de hardware como: Raspberry PI, Arduinos y demás para ejecutar intrusiones informáticas demostrando que los mismos se pueden hacer tales como lo hacen las herramientas de software instaladas en Windows, realizando ataques aplicando las placas electrónicas. Desde la aparición del Raspberry PI con el transcurso del tiempo se han ido presentando proyectos tecnológicos de toda índole con el objetivo de promover la innovación y la investigación aumentando así el conocimiento científico-tecnológico en las personas.

Debido a la optimización de recursos computacionales surge la necesidad de emplear auditorías de seguridad informática a través de dispositivos hardware que generen rapidez en el momento de ejecutar una intrusión y que cumplan la misma función de identificar y explotar vulnerabilidades como lo ejecutan los softwares tradicionales con el objetivo de detectar riesgos y aplicar el respectivo tratamiento de estos evitando la no provocación de incidentes de seguridad que conlleve a la perdida de información crítica.

Los mini hardware empiezan a sentirse a nivel mundial, debido a la globalización y a la optimización de recursos computacionales. La primera vez que se veía un producto de hardware y software libre a nivel de aprendizaje y diseño electrónico se dio con las placas Arduino de procedencia italiana. Los Arduinos en su interior incorporan un programador de microcontroladores AVR de conexión USB, donde estos poseen la capacidad de programar el microcontrolador que lleva incorporado en ella a través de un lenguaje de programación basado en C. El departamento de investigación fue el encargado de desarrollar aplicaciones y verificar la factibilidad de trabajo, arrojando como resultado que la integración electrónica y las aplicaciones que se podían hacer con

estas placas superaba al trabajo de usar micro controladores PIC o AVR de la forma tradicional. En caso los Raspberry PI se inician en Reino Unido donde estos son placas de bajo costo, en lo cual incorporan interfaces USB (Universal Serial Bus) que cumplen la función de conectar periféricos de entrada como mouse y teclado e interfaz HDMI (Interfaz Multimedia de Alta Definición) para la conexión de monitores y televisores Smart, además integran una tarjeta de memoria para el almacenamiento del sistema operativo ya que estos trabajan con distribuciones de Linux a diferencia de los Arduinos que son programables, también los Raspberry contienen puertos RJ45 y tarjetas inalámbricas WIFI para la conexión a la red de internet, permitiendo actualizaciones.

A continuación, se presentará lo que se va a desarrollar en cada capítulo del proyecto de titulación:

En el capítulo I, se analizará la situación actual del problema referente a las vulnerabilidades en ordenadores que se conectan a una red de datos, también se determinan los objetivos propuestos, justificar la problemática y delimitar el alcance del proyecto.

En el capítulo II, comprende el marco teórico donde se investigan los antecedentes de proyectos previos, se explicará acerca de la herramienta Poisontap y su modo de conexión con los ordenadores y el tipo de ataque que esta efectúa.

En el capítulo III, se planteará la propuesta tecnológica con sus respectivas etapas de metodología del proyecto, los entregables del proyecto y los criterios de validación de la propuesta.

En el capítulo IV, se presentará los criterios de aceptación del producto o servicio determinando el cumplimiento de los alcances y de los objetivos específicos.

1. CAPÍTULO I

1.1 EL PROBLEMA

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 UBICACIÓN DEL PROBLEMA EN UN CONTEXTO

Hoy en día el uso de las tecnologías de la información y el desarrollo de las telecomunicaciones han evidenciado la importancia que esto infiere en todo el mundo, el creciente avance de la ciencia hacen que muchos de los dispositivos electrónicos se adapten a los requerimientos y las nuevas tendencias de la actualidad, sabemos que todo sistema no es 100% confiable tales como: aplicaciones de casas comerciales, hospitales y demás, por el cual es indudable que día a día los riesgos son mayores por la falta de inversión en seguridad informática por parte de organizaciones que se dedican al ámbito educativo, constructoras, etc. con el objetivo de disminuir y controlar amenazas que afecten a la confidencialidad e integridad de la información, estas vulnerabilidades se hacen presente en todo momento donde algunas empresas obtienen pérdidas económicas de sus activos a causa de ataques cibernéticos como la intercepción de tráfico e inyección de códigos maliciosos para la extracción de datos.(González, 2016)

La información es uno de los activos de vital importancia para las organizaciones donde por medio de la aplicación de métodos de seguridad informática se intenta que los datos sean confidenciales, íntegros y disponibles a personas autorizadas de las compañías que manejen registros de carácter crítico. Lo ideal es que los usuarios corporativos tengan conocimiento de las posibles vulnerabilidades expuestas en los sistemas instalados en ordenadores o estaciones de trabajo para la toma de medidas preventivas que ayuden a contrarrestar las intrusiones maliciosas que circulan por medio de la red.

Actualmente los usuarios que efectúan las tareas de trabajo por medio de ordenadores conectados a una red empresarial son víctimas de ataques informáticos tales como activos y pasivos, debido a esto el personal corporativo ha sugerido aplicar normas de seguridad para la precaución de los posibles riesgos que pueden presentarse en el momento, ya que ellos almacenan información confidencial en las estaciones de trabajo y navegan por la red de una manera excesiva sin tomar en consideración que los datos personales pueden estar expuestos a cualquier tipo de amenaza, por lo cual algunos de los usuarios que poseen conocimiento de Hardware y Software utilizan las placas electrónicas conocidas como Raspberry Pi, Keylogger entre otras, para ejecutar capturas de trafico de internet generado por las personas que se conectan a la red afectando el secreto e integridad de la información en beneficio propio, con la finalidad de ocasionar daños a los activos de la organización logrando que las compañías posean un nivel de confiabilidad demasiado bajo.

1.2.2 SITUACIÓN CONFLICTO. NUDOS CRÍTICOS

La problemática actual surge en algunos de los componentes instalados en computadoras de escritorio, servidores y Laptops, que se encuentran situados en la empresa Marcelo Rúales, disponibles para cualquier conexión logrando que se efectué un ataque informático utilizando placas electrónicas con el objetivo de capturar datos sensibles para ser usados para actividades ilícitas beneficiándose económicamente ocasionando daños en la organización que maneja información crítica.

1.2.3 CAUSAS Y CONSECUENCIAS DEL PROBLEMA

Tabla No. 1 Causas y Consecuencias

La no obtención de un antivirus actualizado.	Produce que los equipos sean mucho más frágiles a cualquier ataque.
No hay inversión en tecnología de seguridad informática.	Produce que existan posibles vulnerabilidades como la extracción de cookies de sesión que pueden ser aprovechadas por atacantes informáticos.
Los componentes USB de los ordenadores no deben ser habilitados en su totalidad.	Ocasiona que pueda haber conexiones de dispositivos electrónicos maliciosos para la captura de datos sensibles.
La Información podría ser capturada fácilmente por crackers debido a las debilidades presentes en los equipos.	Se ocasionaría porque la información confidencial se encuentra expuesta públicamente.

Fuente: Trabajo de Investigación
Autores: Diana Cují-Danilo Jalca

1.2.4 DELIMITACIÓN DEL PROBLEMA

Tabla No. 2 Delimitación del problema

Campo	Hacking de Ordenadores conectados a la red.
Área	Seguridades de redes informáticas.
Aspecto	Dispositivos Electrónicos.
Tema	Análisis de las vulnerabilidades de la red de datos de la empresa PYME “Marcelo Rúales” de la ciudad de Guayaquil, utilizando la herramienta POISONTAP para el Hacking ético e inyección de puertas traseras y captura de tráfico HTTP-HTTPS, incorporando las recomendaciones necesarias para su mitigación.

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

1.2.5 FORMULACIÓN DEL PROBLEMA

- Los riesgos que se producirían al momento que se perpetúe un ataque informático ocasionan que personas maliciosas con conocimiento en seguridad puedan acceder a la información confidencial de la compañía con el objetivo de beneficiarse económicamente.

- Una de las amenazas que puede producir los atacantes es la toma de control total de la información ocasionando daños irreversibles a los activos tanto físicos y lógicos.

- Otros de los riesgos que se puede producir por parte de los crackers es que una vez que accedan a la confidencialidad de la información puedan realizar copias de seguridad de los datos sensibles sustrayendo los ficheros en beneficio propio.

EVALUACIÓN DEL PROBLEMA

Los aspectos por considerar dentro del proyecto de titulación a desarrollar son los siguientes:

- **Delimitado:** La problemática que se puede identificar en los ordenadores que poseen varios componentes en su placa madre que se encuentran habilitados como los puertos USB, donde los atacantes pueden establecer una conexión para la captura de los datos sensibles.

- **Concreto:** Por medio de la herramienta Poisontap se analizará las vulnerabilidades aplicando las fases de un Hackeo ético con el objetivo de dictaminar recomendaciones para mitigar y tomar el control de los riesgos expuestos en cada fallo de seguridad.

- **Original:** El proyecto de investigación a desarrollar demuestra la originalidad debido a que la herramienta que se utilizara para realizar las pruebas de Hackeo ético es novedosa y presenta avances tecnológicos como establecer conexiones de red por medio del puerto USB.

- **Contextual:** La información es de vital importancia por lo cual al no contar con mecanismos de seguridad que permitan salvaguardar la confidencialidad, integridad y disponibilidad de los datos da lugar a que crackers se puedan apoderar de los activos lógicos produciendo perdidas a las organizaciones.

- **Factible:** La herramienta que se utilizara para realizar las pruebas de Hackeo ético es una placa electrónica de bajo costo llamada Poisontap que se la aplicara para la captura de tráfico http-https y la inyección de puertas traseras.

- **Identifica los productos esperados:** Una vez realizadas las pruebas de Hackeo ético por medio de la herramienta Poisontap se aplicará las medidas de seguridad para su respectiva mitigación de vulnerabilidades encontradas.

1.2.6 OBJETIVOS

1.2.7 OBJETIVO GENERAL

Analizar las vulnerabilidades de la red de datos de la empresa pyme “Marcelo Rúales” de la ciudad de Guayaquil utilizando la herramienta Poisontap para el hacking ético e inyección de puertas traseras y captura de tráfico http-https, para determinar las recomendaciones necesarias y poder tomar las medidas de seguridad adecuadas.

1.2.8 OBJETIVOS ESPECÍFICOS

1. Realizar un levantamiento de información de la red detallando los dispositivos y ordenadores con su respectivo direccionamiento IP que conforman dicha red y esquemas de seguridad implementados proporcionando un diseño de esta.

2. Realizar simulaciones de ataques informáticos por medio de la herramienta Poisontap y aplicando las fases de un Hackeo ético inyectando puertas traseras en servidores Windows y la captura de tráfico http-https.

3. Emitir las medidas de solución pertinentes en base a las vulnerabilidades USB explotadas, para que la empresa pueda tener una seguridad informática adecuada.

ALCANCES DEL PROBLEMA

El alcance del problema consiste en realizar un levantamiento de información de la red detallando los dispositivos, ordenadores, esquemas de seguridad implementados y direccionamiento IP de la empresa pyme Marcelo Rúales para en base a la información recopilada ejecutar las pruebas de Hackeo ético por medio de la herramienta Poisontap, para finalmente presentar un informe especificando los resultados obtenidos durante el análisis de vulnerabilidades y proponiendo las correcciones para mitigar las medidas de los riesgos encontrados.

JUSTIFICACIÓN E IMPORTANCIA

Con el análisis de vulnerabilidades por medio de la herramienta Poisontap se dará a conocer a la empresa pyme “Marcelo Rúales” los fallos de seguridad que puede tener los ordenadores conectados a una red y como se puede hacer un mal uso de ellas con la finalidad de tomar planes de acción y de contingencia para el tratamiento de los riesgos presentes en cada falencia.

Además, la herramienta Poisontap dará a conocer la importancia de proteger la información sensible ante ataques informáticos por medio de pruebas de Hackeo ético aplicando la placa electrónica Poisontap.

METODOLOGÍA DEL PROYECTO

La metodología del proyecto de titulación a desarrollar comprende 3 únicas fases que se detallaran a continuación.

- **Fase 1:** En esta fase se realizará un levantamiento de información de la red detallando los dispositivos, ordenadores, direccionamiento IP y esquemas de seguridad implementados de la empresa Pyme Marcelo Rúales.

- **Fase 2:** En esta segunda fase se realizarán las pruebas de Hackeo ético por medio de la herramienta Poisontap para diagnosticar las vulnerabilidades presentes identificando sus riesgos.

- **Fase 3:** En esta última fase se presentará un informe detallando los resultados obtenidos de las pruebas de Hackeo ético.

2. CAPÍTULO II

2.1 MARCO TEÓRICO

2.1.1 ANTECEDENTES DEL ESTUDIO

Actualmente en el Ecuador se han hecho evidente los avances tecnológicos en gran magnitud, el uso de las tecnologías de la información ha logrado que los usuarios sean más eficientes en el momento de ejecutar tareas específicas que son asignadas por las organizaciones de carácter público o privado generando un mejor rendimiento en las personas al instante de ejercer una actividad.(Granda, 2016)

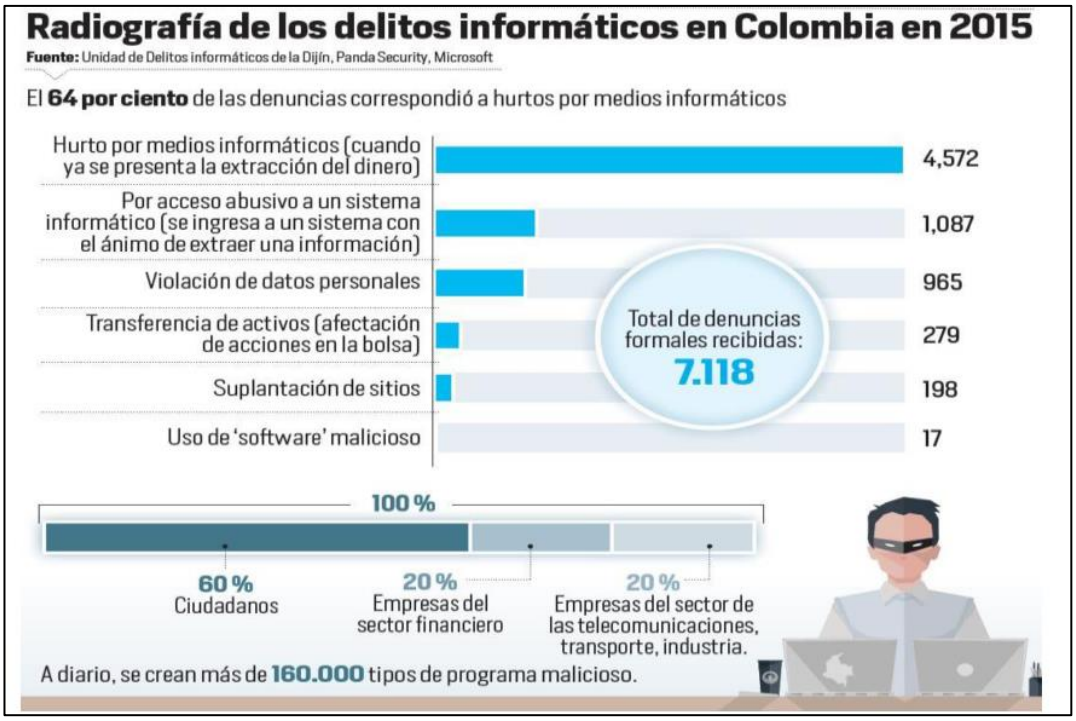
Hoy en día es evidente que la seguridad informática es la preocupación principal de las organizaciones más aún cuando los datos sensibles son expuestos en el internet, por estas razones es de vital importancia que se realicen análisis de vulnerabilidades en las redes de datos para verificar los tipos de riesgos y amenazas que pueden comprometer que la información pueda sufrir daños irreversibles.(Granda, 2016)

Según un estudio realizado por los estudiantes de la carrera de Ingeniería en Networking y Telecomunicaciones Lidia Álvarez y Félix Anzules en su proyecto de titulación desarrollado en el año 2017 detallan que actualmente profesionales de seguridad informática han desarrollado aplicaciones para encriptar la información cuando esta es enviada a un destinatario mediante la red de internet creando tuéneles de comunicación cifrados con el objetivo de disminuir los índices de vulnerabilidades expuesto en las redes y establecer toma de control de riesgos para finalmente mantener los datos protegidos.(Coello & Alejandrina, 2017)

En Colombia país vecino de Ecuador aún no se reconoce el Hackeo ético a nivel profesional por lo tanto las tres áreas laborales en la cual trabajan los profesionales de seguridad informática son en empresas dedicadas a la auditoría de redes, departamentos de sistemas o ejercen actividades comerciales referentes al Hackeo fuera de horarios de trabajo.(Himanen, 2013)

En Colombia diferentes medios de comunicación escrita en el año 2015 como el caso del periódico el tiempo verificar el gráfico No. 1, detalla en una radiografía los delitos informáticos que se han efectuado a personas de índole público y privado donde por medio de unidades especializadas como el grupo DIJIN de la Policía Nacional, suministran información real sobre los incidentes de seguridad perpetuados donde se generaron perdidas económicas equivalentes a $600 millones de dólares en dicho país.(Antonio, Forero, Manuel, & Garcia, 2016)

Gráfico No. 1 Delitos Informáticos en Colombia



Fuente: http://www.eltiempo.com/archivo/documento/CMS-16493604
Autor: Diario el Tiempo

En un estudio realizado por diario el tiempo muestra en forma real como se efectúa el hurto de datos confidenciales por medio de dispositivos informáticos ejecutando intrusiones maliciosas a sistemas bancarios para el acceso a los registros de cada cliente, convirtiéndolo en uno de los delitos más comunes en Colombia. El 64% de las denuncias generadas ante autoridades judiciales mencionan las pérdidas de información como números de tarjeta de crédito, números de cuentas bancarias, cedulas de identidad y demás.(Tiempo, 2015)

Según diario El Universo el 26 de noviembre del año 2013 detalla que clientes de varias entidades bancarias utilizaron las redes sociales para denunciar delitos informáticos referente a la clonación de tarjetas de débito y crédito, donde los usuarios se percataron del delito por medio de mensajes de texto SMS, avisos por parte de cajeros de supermercados mencionándoles que la tarjeta no poseía el saldo suficiente para realizar una compra y también realizando la verificación de saldo en la página web de las instituciones financieras.(Universo, 2013)

2.1.2 FUNDAMENTACIÓN TEÓRICA

Test de Intrusión

El test de intrusión es un procedimiento que se ejecuta a través de un conjunto de técnicas y métodos que simulan un ataque cibernético a un sistema o toda una red, este tipo de testing es aplicado para evaluar la seguridad de una organización detallando su estado actual para poder tomar las medidas preventivas con el objetivo de mitigar las amenazas que se propagan por la red de datos.(Ramos Ramos, 2014)

Las herramientas que se incluyen en el momento de realizar un test de penetración son las siguientes:

- Escaneo de puertos por NMAP.
- Test de intrusión a sistemas y redes, aplicando ataques de fuerza bruta por medio de aplicaciones de hydra y medusa.
- Sniffing de redes y penetración de firewalls aplicando herramientas de análisis de tráfico como Wireshark y Ettercap.
- Escaneo de vulnerabilidades en aplicaciones Web por medio de aplicaciones de W3AF, OWASP ZAP PROXY y demás.

Tipos de PENTESTING

Para realizar pruebas de penetración a sistemas informáticos o infraestructuras de red instaladas en empresas de carácter público y privado se consideran las siguientes fases que se detallan a continuación verificar el gráfico No. 2:

Fase de descubrimiento

Esta fase consiste en delimitar las áreas donde será enfocada para ejecutar la evaluación de seguridad en la red de una empresa, para efectuar esta fase el auditor de seguridad informática debe de comprender los riesgos que se asocian a la línea de negocio basado en el uso de los activos de información.(Ramos Ramos, 2014)

A continuación, se detallará el tipo de información que el hacker ético recopila para cumplir esta fase de un test de penetración.

- Rango de direccionamiento IP asignado a estaciones de trabajo y servidores.
- Cuentas de correo electrónico.
- Análisis de las aplicaciones Web.
- Detección de redes inalámbricas.
- Servicios asociados al dominio.

Fase de exploración

En esta fase del test de penetración se enfoca en identificar todos los blancos potenciales para poder efectuar un ataque cibernético explotando algunas de las vulnerabilidades consideradas de vital importancia por los piratas informáticos.(Ramos Ramos, 2014)

Además, se integra el análisis de protocolos de redes de datos, relevamiento de plataforma y mecanismos de protección, escaneo de redes telefónicas, detección de puertos TCP y UDP en estado abierto, localización remota de servicios basados en Linux y Windows y sistemas operativos clientes y búsqueda de vulnerabilidades en aplicaciones web.(Ramos Ramos, 2014)

Las tareas que son parte de esta fase son las siguientes:

- Detección de dispositivos de red y versiones de sistemas operativos clientes y servidores Linux y Windows.
- Localización de puertos TCP y UDP en estado abierto.
- Identificación de vulnerabilidades en servidores Web.
- Rango de direccionamiento IP.

Fase de evaluación

En esta etapa se evalúa todas las vulnerabilidades expuestas en los sistemas operativos y servicios localizados en la fase anterior, pudiendo verificar que fallos de seguridad puedan comprometer la información almacenada en las plataformas de usuarios. Durante la fase de evaluación se realizan las siguientes tareas que se mencionan a continuación.(Ramos Ramos, 2014)

- Ejecución de herramientas de escaneo de vulnerabilidades.
- Búsqueda manual de fallos de seguridad.

Fase de intrusión

En esta última etapa se la denomina la más compleja del test de penetración donde el auditor de seguridad informática ejecuta ataques cibernéticos para determinar los tipos de riesgos que contienen cada vulnerabilidad identificada en procesos anteriores.(Ramos Ramos, 2014)

Gráfico No. 2 Test de intrusión

Fuente: https://slideplayer.es/slide/12487168/
Autor: José Quispe Palacios

Ataques físicos

Ingeniería social

La ingeniería social es uno de los ataques más utilizados por los crackers para establecer accesos a los sistemas informáticos y a redes corporativas logrando aplicar técnicas de engaño a usuarios con poco conocimiento de informática verificar gráfico No. 3, además la ingeniería social se la aplica solamente a personas con mayor confiabilidad en otros individuos donde los atacantes se ganan la confianza con el objetivo de recopilar la información de la organización, también este ataque se lo

pueden efectuar realizando llamadas por teléfono a personas con privilegios de acceso a los sistemas de información y comunicación.(Mieres, 2013)

Como contramedida a los ataques de ingeniería social, es aplicar un sistema de educación superior a usuarios sobre el manejo de sistemas informáticos y políticas empresariales con la finalidad de que estos puedan dejar de ser víctimas de atacantes que tienen como objetivo acceder a la confidencialidad de la información de las compañías que manejan datos críticos.(Mieres, 2013)

Gráfico No. 3 Ingeniería Social

Fuente: (Mieres, 2013)
Autor: Jorge Mieres

Los ataques físicos se clasifican de la siguiente manera:

- Desastres naturales, incendios y tormentas o inundaciones.
- Sabotaje interno y externo de forma deliberada.
- Ruido eléctrico.

Incendios

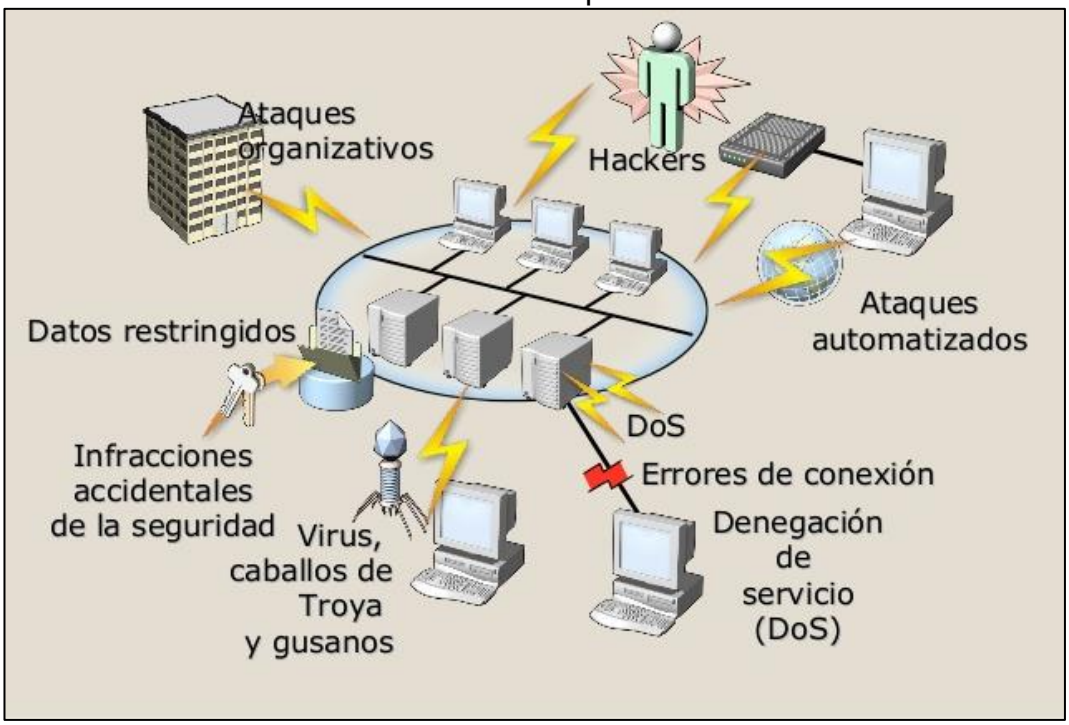
Los incendios son producidos por el uso inadecuado dispositivos de redes que son alimentados por corrientes eléctricas donde la falta de mantenimiento de equipos electrónicos ha generado que los mismos se

sobrecalienten llegando a ocasionar incendios de forma accidental. Además, ciertos ataques informáticos pueden provocar incendios en las instalaciones del centro de datos de una empresa.

Como poder evitar los incendios:

- El centro de cómputo de las empresas debe tener extintores.
- Utilizar piso falso en las instalaciones.
- Aplicar medidas para evitar que los usuarios fumen en áreas donde se pueden provocar incendios.

Gráfico No. 4 Ataques físicos



Fuente: https://es.slideshare.net/contiforense/delito-y-fraude-informtico-4667430

Autor: UNIVERSIDAD CONTINENTAL

Seguridad física

Las principales amenazas presentes en un sistema informático instalado en una compañía son los desastres naturales, incendios accidentales, tormentas, temperaturas extremas, terremotos e inundaciones que

generan grandes consecuencias catastróficas; debido a que también se presentan amenazas ocasionadas por el usuario tales como los disturbios, sabotajes internos o externos en forma deliberada, etc. La seguridad física tiene la capacidad de prevenir cada una de estas anomalías producidas por personas malintencionadas cuyo objetivo es causar daños a los activos de información.(Ochoa, 2013)

La seguridad física del entorno consiste en aplicar barreras físicas como se ve en el gráfico No. 5 y procedimientos de control, para poder prevenir las amenazas y su vez logrando mitigar los posibles riesgos que puedan comprometer la información con el objetivo de que esta se mantenga confidencial.(Ochoa, 2013)

Gráfico No. 5 Seguridad Física

Fuente: http://caroline00317.blogspot.com/2012/11/seguridad-fisica-de-un-centro-de-computo.html
Autor: GABRIELA CAROLINA GONZÁLEZ

Detallando las principales amenazas, vulnerabilidades y ataques se aplica un esquema de protección para prevenir posibles riesgos generados por amenazas de carácter interno y externo, con el fin de establecer una detección y así mismo ejecutar las medidas de control adecuadas cumpliendo las políticas de seguridad.(Ochoa, 2013)

Las medidas de seguridad que se recomiendan son las siguientes:

- Realizar actualizaciones en los sistemas operativos clientes y mantener seguros los ordenadores aplicando contraseñas de accesos fuertes.
- Los administradores de tecnológica deben configurar la red de forma adecuada.
- Tener conocimiento de cada una de las posibles vulnerabilidades que pueden comprometer la información sensible por medio de un ataque.
- Implementar una gestión sobre el manejo de incidentes de seguridad y la forma como prevenirlos.
- Aplicar estándares de seguridad informática como la ISO 27001 para la implementación de controles que ayuden a disminuir los posibles ataques cibernéticos.

Herramientas para realizar ataques físicos en organizaciones

Keylogger

Los Keylogger son programas informáticos en lo cual estos registran las pulsaciones que realizan los usuarios por medio del teclado de una computadora para después ser almacenadas en un archivo o enviadas

por medio de la red de internet. El objetivo de un Keylogger es ser una aplicación maliciosa para quien lo instale en un ordenador lo hace de forma oculta incluso saber lo que escriben los usuarios. También existen softwares malintencionados que los contiene un Keylogger como troyanos o gusanos.(Palomeque, 2013)

Tipos de Keylogger

- **Keylogger por hardware:** Son dispositivos que se conectan al ordenador por medio del puerto USB con el objetivo de registrar las pulsaciones por teclado verificar gráfico No. 6.
- **Keylogger por software:** Son aplicaciones espías que son instaladas en sistemas operativos Windows para la captura de datos que son generadas por los usuarios.

Gráfico No. 6 Keylogger

Fuente: https://markuta.com/keygrabber-nano-usb-keylogger-review/
Autor: MARKUTA

Desbloqueo de dispositivos inteligentes desde un Android

Para proceder a desbloquear dispositivos los atacantes utilizan la depuración ADB donde se conecta el Android con el ordenador mediante cable USB como se ve en el gráfico No. 7.

Ventajas de ADB (ANDROID DEBUG BRIDGE)

- ADB ejecuta aplicaciones cuando el dispositivo Android este bloqueado por una contraseña o sensor de huellas dactilares.
- ADB es utilizado por los programadores para la ejecutar pruebas en las aplicaciones en el dispositivo Android conectado por USB.
- Por medio de ADB se puede rootear o aplicar el súper usuario a un dispositivo Android.
- ADB también aplica borrado de patrones de acceso a los dispositivos móviles Android.

Gráfico No. 7 Android ADB

Fuente: http://androidspan.ru/cmo/5034-personalizacin-de-android-cmo-transferir-archivos.html
Autor: Android Span

POISONTAP

Características de POISONTAP

- Emula un dispositivo Ethernet por medio del puerto USB.
- Captura todo el tráfico de la red de internet generado por el ordenador.
- Almacena las cookies y sesiones HTTP del navegador Web instaladas en el ordenador.

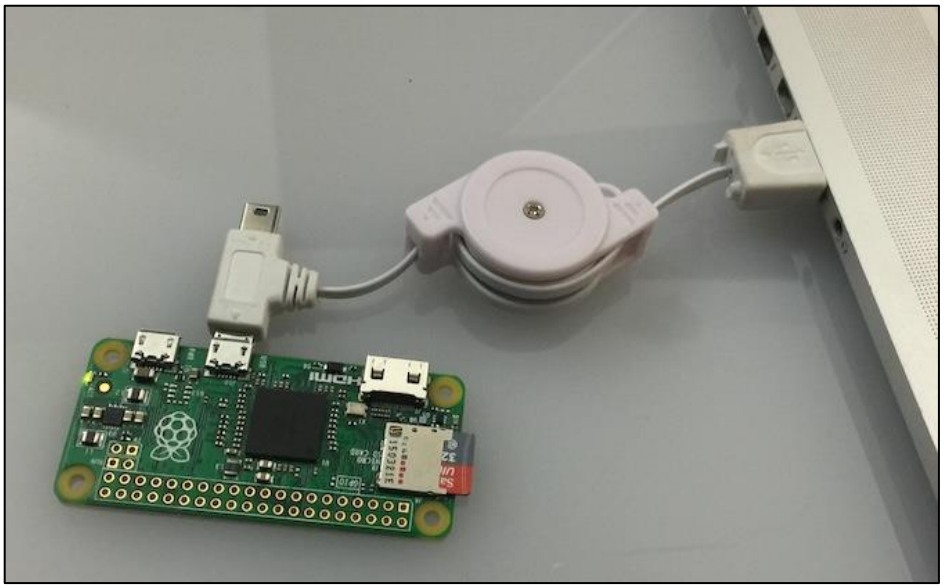
- Expone el enrutador interno que provee la conexión a internet a los atacantes.
- Instala una puerta trasera persistente basada en la Web en la cache del protocolo HTTP.
- No requiere que el ordenador sea desbloqueado.

Mecanismos de seguridad que evade POISONTAP

- Pantalla de bloqueo protegidas por contraseñas.
- Prioridad de tabla de enrutamiento e interfaz de red de origen.
- Autenticación de dos factores y factores múltiples.
- Protección de cookies HTTPS.

POISONTAP está diseñado para realizar ataques físicos por medio de una RASPBERRY PI ZERO con el objetivo de interceptar y vulnerar ordenadores conectados a una red de datos a través de esto capturar información sensible véase gráfico No. 8.

Gráfico No. 8 POISONTAP



Fuente: https://samy.pl/poisontap/
Autor: SAMY KAMKAR

Ataques que se pueden realizar por medio POISONTAP

- El atacante se conecta al ordenador POISONTAP (como Raspberry Pi Zero armado) en un ordenador bloqueado (incluso si la computadora está protegida con contraseña).

- POISONTAP es un dispositivo o placa electrónica que emula un dispositivo Ethernet (por ejemplo, Ethernet sobre USB / Thunderbolt): de forma predeterminada, Windows, OS X y Linux reconocen un dispositivo Ethernet, lo cargan automáticamente como un equipo de red de baja prioridad y realizan una solicitud DHCP a través de él, incluso cuando la máquina está bloqueada o protegida con contraseña.

- POISONTAP responde una solicitud DHCP proporcionando a la máquina una dirección IP privada; sin embargo, la respuesta DHCP está diseñada para indicarle a la máquina que todo el espacio IPv4 (0.0.0.0 - 255.255.255.255) es parte de la red local de POISONTAP, en lugar de una pequeña subred (por ejemplo, 192.168.0.0 - 192.168.0.255).

Puertas traseras basadas en servidores web que se accesibles remotamente

- POISONTAP produce miles de iframes, obligando al navegador a cargar cada uno, estos no en lo cual no son solo páginas en blanco, sino más bien puertas traseras HTML + JavaScript que se almacenan en la memoria cache indefinidamente.

- La placa electrónica POISONTAP almacena estas puertas traseras en cada dominio sea empresarial o de origen doméstico, la puerta trasera está ligada a ese dominio, lo que permite al pirata

informático utilizar las cookies del dominio e iniciar solicitudes de origen idéntico en el futuro, incluso si el usuario no está conectado actualmente.

- Por ejemplo, cuando el usuario efectúa una carga el http://nfl.com/PoisonTap iframe, POISONTAP acepta el tráfico de Internet desviado, responde a la solicitud HTTP a través del servidor web Node.

- Se agregan encabezados HTTP adicionales para almacenar en caché la página indefinidamente.

- La respuesta de la solicitud realizada por el usuario a la página es una combinación de HTML y JavaScript produciendo un WebSocket persistente en el servidor web del atacante por medio de la red de internet.
  - El WebSocket permanece abierto y permite al atacante, en cualquier momento, conectarse de nuevo a la máquina por medio del backdoored con el objetivo de realizar solicitudes desde cualquier origen que tenga la puerta trasera implementada.

  - Nuevamente, cualquier opción de "X-Frame-Options", Cross-Origin Resource Sharing y Same-Origin Policy en el dominio se pasa por alto por completo ya que la solicitud golpeará el caché que dejó POISONTAP en lugar del dominio verdadero.

Archivos de configuración de Poisontap

- **pi_poisontap.js** – Este archivo se ejecuta por medio del Node.js en la Raspberry Pi Zero en donde el servidor HTTP cumple con la funcionalidad de manejar cualquier solicitud HTTP interceptada por

Poisontap en un ordenador, almacenando las cookies de sesión de usuarios e inyectar las puertas traseras almacenadas en caché.

- **pi_startup.sh**: Se ejecuta una vez iniciado el Raspberry Pi Zero donde se configura el dispositivo con el objetivo de emular un dispositivo Ethernet sobre USB, estableciendo un servidor DHCP malicioso, permitiendo el redireccionamiento del tráfico, la suplantación DNS y el lanzamiento de pi_poisontap.js encima.
- **target_backdoor.js**: Este archivo se antepone a cualquier archivo JavaScript relacionado con CDN, como los backdooring, la URL jQuery de Google CDN.
- **poisontap.cookies.log**: Este archivo se genera una vez que la máquina del usuario comienza a enviar solicitudes HTTP a Poisontap y registra la cookie desde el navegador junto con la URL / dominio asociado al que pertenece.

Mecanismos de seguridad que evade Poisontap

Tabla No. 3 Métodos de Protección que evade Poisontap

Computadoras protegidas con contraseña
Prioridad de tabla de enrutamiento
Sistemas informáticos con doble y múltiple factor de autenticación
DNS Pinning
Protección de cookies HTTPS

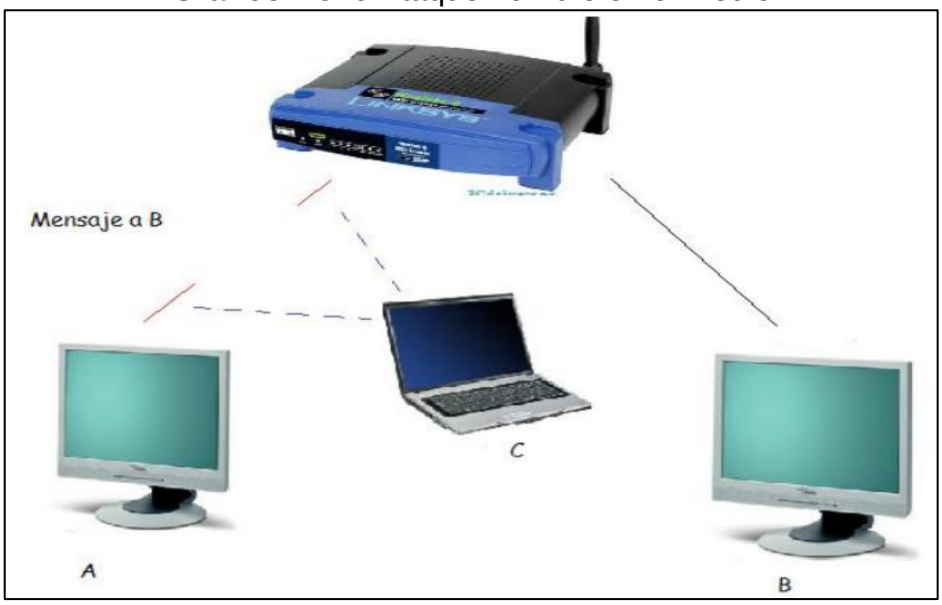
Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Ataque hombre en el medio

El ataque hombre en el medio es una intrusión pasiva que permite la captura de tráfico que circula en una red de datos sea Ethernet o inalámbrica como se ve en el gráfico No. 9, este ataque también posee la capacidad de capturar sesiones de usuarios y credenciales de acceso a los sistemas informáticos.(David Galisteo, 2012)

A continuación, se muestra un ejemplo del ataque hombre en el medio.

Gráfico No. 9 Ataque hombre en el medio



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Virus informáticos que infectan el ordenar por medio de una unidad de almacenamiento

Tabla No. 4 Virus informáticos

Malware	Descripción
RECYCLER	Consiste en crear un acceso directo a una aplicación eliminando el programa original.
TROYANO	Consiste en sustraer información o producir daños en el sistema del Hardware.
BOMBAS LÓGICAS	Son aplicaciones que se activan por medio de acontecimientos que se dan en un periodo determinado.
GUSANO	Cumple la función de duplicarse así mismo.
HOAX	Son mensajes de contenido falso que incitan al usuario a realizar copias de seguridad y enviarlas a sus contactos.
JOKE	Es una página pornográfica que se el usuario llega a cerrarla provoca que exista un mensaje de error.
BACKDOORS	Son puertas traseras que al ser activadas en el ordenador el cracker toma el control total del mismo.

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Listado de antivirus

Tabla No. 5 Lista de antivirus

Antivirus	Descripción
NORTON	Este antivirus detecta códigos maliciosos desde el internet disminuyendo la infección de los ordenadores.
KAPERSKY	Posee un gran desempeño en la detección de malware protegiendo a los usuarios que se conectan a la red de internet e intranet.
AVG	Es un antivirus de bajo costo donde su principal función es desinfectar los ordenadores de códigos maliciosos eliminando las posibles amenazas.
PCTOOLS	Este antivirus requiere de ayuda en línea para efectuar un gran desempeño.
BITDEFENDER	Provee una fuerte protección a los usuarios previniendo los riesgos que pueden afectar a la información.
AVAST	Este antivirus posee algunas funciones para la seguridad de internet donde emite alertas sobre amenazas y troyanos en lo cual procede a bloquearlos automáticamente.
MACAFEE	Posee gráficos únicos y actualizados los que hacen mejor que los demás antivirus.
PANDA SECURITY	Provee todas las funciones básicas de seguridad, es muy seguro con los dispositivos USB conectados al ordenador.

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

2.1.3 FUNDAMENTACIÓN LEGAL

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

SECCIÓN VIII

CIENCIA, TECNOLOGÍA, INNOVACIÓN Y SABERES ANCESTRALES

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrán como finalidad:

Generar, adaptar y difundir conocimientos científicos y tecnológicos.

Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Art. 386.- El sistema comprenderá programas, políticas, recursos, acciones, e incorporará a instituciones del Estado, universidades y escuelas politécnicas, institutos de investigación públicos y privados, empresas públicas y privadas, organismos no gubernamentales y personas naturales o jurídicas, en tanto realizan actividades de investigación, desarrollo tecnológico, innovación.

Código orgánico integral penal

SECCIÓN TERCERA

Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Art. 178 Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona tiene una pena privativa de 1 a 3 años.

Artículo 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el

interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar

de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Artículo 233.- Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

LEY DE COMERCIO ELECTRONICO

Art. 5.- Confidencialidad y reserva. - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Art. 9.- Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

HIPÓTESIS

1. ¿Cree usted que por medio de la herramienta POISONTAP la empresa Marcelo Rúales podrá conocer los riesgos que podría producir la placa electrónica al ser utilizada para fines maliciosos?

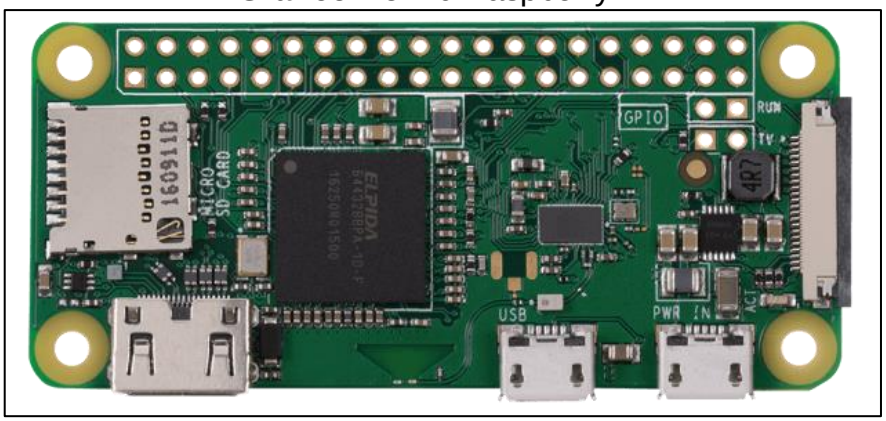
2. ¿Considera usted que es de vital importancia realizar un test de penetración en la empresa Marcelo Rúales para diagnosticar las posibles vulnerabilidades y poder tomar las medidas de seguridad adecuadas?

3. ¿Ha pensado usted que la placa electrónica RASPBERRY PI ZERO pueden ser un gran peligro para la información cuando es utilizada para fines maliciosos?

2.1.4 DEFINICIONES CONCEPTUALES

RASPBERRY PI: Se lo denomina un computador de placa reducida como se ve en el gráfico No. 10, u ordenador de placa simple de bajo costo desarrollado en el Reino Unido por la fundación RASPBERRY PI con el objetivo de estimular las enseñanzas de las ciencias de la computación.

Gráfico No. 10 Raspberry PI



Fuente: http://market.samm.com/raspberry-pi-zero-w-en
Autor: SAMM MARKET

Hacker: Persona experta en algún campo de la informática donde esta sus conocimientos de hacking con fines defensivos y legales para que las empresas no puedan ser víctimas de ataques cibernéticos proporcionados por los crackers.

Cracker: Persona que utiliza los conocimientos de la informática para ocasionar daños a las redes de las empresas con el objetivo de beneficiarse económicamente. Además, también se los denomina piratas cibernéticos.

Amenaza: Potencial de ocurrencia de un hecho que pueda manifestarse en lugar específico generando temor en los usuarios y con la posibilidad de poder comprometer la confidencialidad e integridad de la información.

Riesgo: Se considera como una probabilidad de que ocurra un hecho o acontecimiento produciendo ciertos efectos en lo cual los datos pueden verse en peligro generando que el atacante malicioso logre tener acceso a la información sensible.

Vulnerabilidad: Las vulnerabilidades son relacionadas con los riesgos y las amenazas en lo cual los crackers al detectar un fallo de seguridad en la red de una compañía la misma puede verse en peligro referente a la perdida de datos sensibles.

3. CAPÍTULO III

3.1 METODOLOGIA DE LA INVESTIGACION

3.1.1 MODALIDAD DE LA INVESTIGACIÓN

La modalidad de la investigación que se empleará en el presente proyecto de titulación en desarrollo referente al análisis de vulnerabilidades en la red de datos de la empresa “Marcelo Rúales” utilizando el miniordenador Poisontap será la de proyecto factible, en donde dicha modalidad se enfoca en la recopilación de información de vital importancia y revisión de material bibliográfico.

3.1.2 TIPO DE INVESTIGACIÓN

Para la implementación de la propuesta tecnológica se emplearán dos tipos de investigación que son las siguientes: investigación campo y documental, en donde se recopilara información del funcionamiento de la placa electrónica PT, el tipo de sistema operativo Linux a instalar y la configuración del Poisontap, con el objetivo de poder realizar un análisis de vulnerabilidades aplicando un ambiente controlado en una red de área local.

En cuanto al trabajo de campo se aplicó como técnica de recolección de datos la encuesta, con el objetivo de medir la viabilidad del proyecto tecnológico, además enfocándose en los posibles riesgos que se pueden presentar se puede determinar que la propuesta es factible para todo tipo de organización que requiere efectuar el análisis de vulnerabilidades.

3.1.3 POBLACIÓN Y MUESTRA

Como población y muestra a la vez se seleccionó un total de 15 personas que laboran en la empresa de los cuales 6 laboran en oficina y 9 en campo y serán participes en la encuesta para iniciar con el proceso de recopilación de información.

3.1.4 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Técnica e instrumentos

Las técnicas que se aplicaran el presente proyecto de titulación en fase de desarrollo es la encuesta que son dirigidas a una muestra representativa equivalente a 15 usuarios que laboran en la empresa.

Se realizarán encuestas a estas 15 personas para determinar la viabilidad del proyecto con el objetivo de demostrar las vulnerabilidades de las estaciones de trabajo a través de la placa PT.

Recolección de la información

Para el proceso de recolección de la información se encuestarán a 15 personas del área con el objetivo de recopilar la mayor cantidad de datos referente a los riesgos y amenazas que se pueden presentar en las redes de datos y a su vez analizar estas inseguridades a través de una placa electrónica Raspberry PI Zero W.

3.1.4 PROCESAMIENTO Y ANÁLISIS

El procesamiento y análisis se lo ejecutará a través del resultado obtenido por las encuestas en base a un total de 15 personas comenzando a interpretar cada ítem, para la tabulación de las preguntas se utilizará la herramienta Microsoft Excel, donde esta permite desarrollar tablas dinámicas y gráficos de pastel para la tabulación de los datos por medio de la utilización de complementos estadísticos integrados en la aplicación de Excel, en este caso el diagrama de barra fue el seleccionado para la representación de salida.

La herramienta Microsoft Excel permite manejar una excelente distribución de la información para un adecuado análisis y compresión de la operación estadística a emplear logrando así la interpretación de datos concretos e ir obtenido los porcentajes de cada pregunta tabulada con el objetivo de sustentar los argumentos y propuestas validas determinando el nivel de aceptación del proyecto de titulación.

Para el procesamiento y análisis se requiere seguir una serie de procedimientos que se detallan a continuación:

1. Se plantearán un total de 8 preguntas.
2. El objetivo por el cual se formuló las preguntas es la determinar el nivel de importancia del proyecto.
3. Elaborar una tabla con la frecuencia detallando los porcentajes de los resultados obtenidos por cada pregunta.
4. Representar gráficamente los porcentajes resultantes de la encuesta por medio de diagrama de barras.
5. Validación de la hipótesis referente a todas las preguntas de encuestas.

3.1.5 ANÁLISIS DE LAS ENCUESTAS

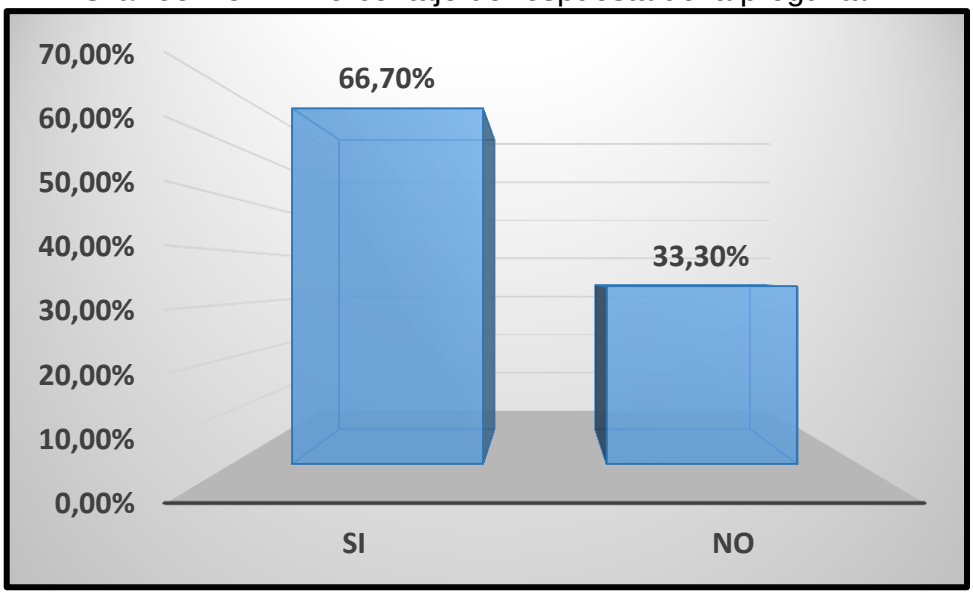
1. ¿Cree usted que con el miniordenador Raspberry PI Zero se podrá identificar amenazas que afecten a la información almacenada en una computadora cliente?

Tabla No. 6 Respuesta de la pregunta 1

Alternativas	Cantidad	Porcentajes
SI	10	66.7%
NO	5	33.3%
Total	15	100.0%

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 11 Porcentaje de respuesta de la pregunta 1



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Análisis: Durante la encuesta realizada se verifico que el 66.7% de los usuarios creen que con el miniordenador Raspberry PI Zero se podrán identificar las amenazas que puedan afectar a la información.

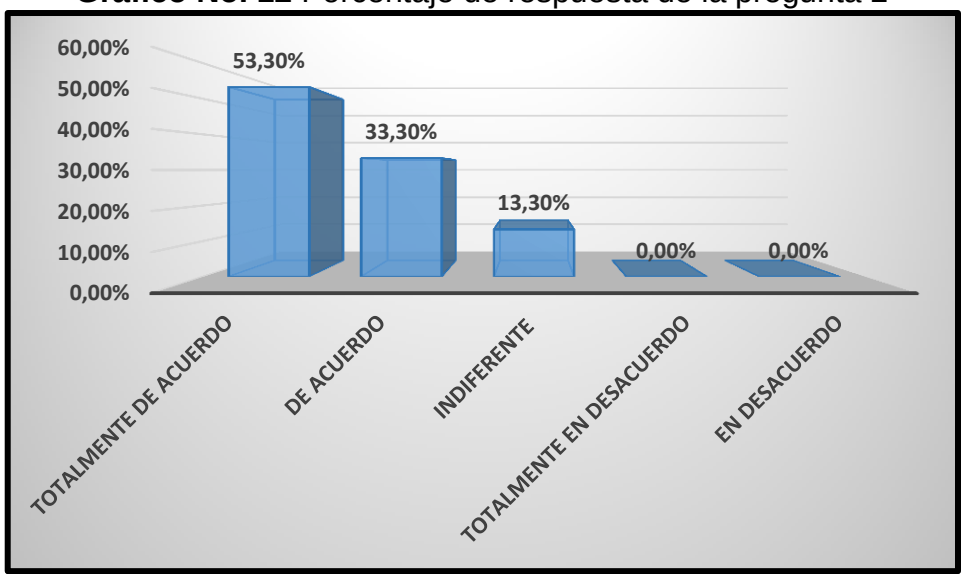
2. ¿Está usted de acuerdo que se realice un análisis de vulnerabilidades por medio de la placa electrónica Raspberry PI Zero W Poisontap para después determinar las medidas de protección?

Tabla No. 7 Respuesta de la pregunta 2

Alternativas	Cantidad	Porcentajes
Totalmente de acuerdo	8	53.3%
De acuerdo	5	33.3%
Indiferente	2	13.3%
Totalmente en desacuerdo	0	0.0%
En desacuerdo	0	0.0%
Total	15	100.0%

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 12 Porcentaje de respuesta de la pregunta 2



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Análisis: Durante la encuesta realizada se verifico que el 53.3% de los usuarios están totalmente de acuerdo que se realice un análisis de

vulnerabilidades con el miniordenador Raspberry PI Zero para determinar las medidas de protección.

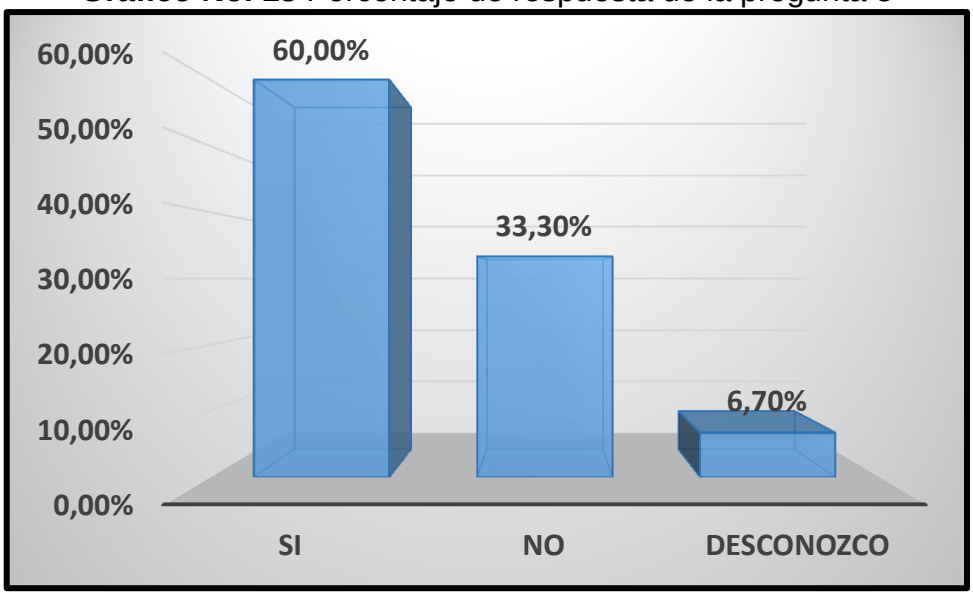
3. ¿Se han producido intrusiones maliciosas a los ordenadores ocasionándole pérdidas de información crítica?

Tabla No. 8 Respuesta de la pregunta 3

Alternativas	Cantidad	Porcentajes
SI	9	60.0%
NO	5	33.3%
Desconozco	1	6.7%
Total	15	100.0%

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 13 Porcentaje de respuesta de la pregunta 3



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Análisis: Durante la encuesta realizada se verifico que el 60.0% de los usuarios detallan que si se han perpetuado intrusiones maliciosas en los ordenadores generando pérdidas de información crítica.

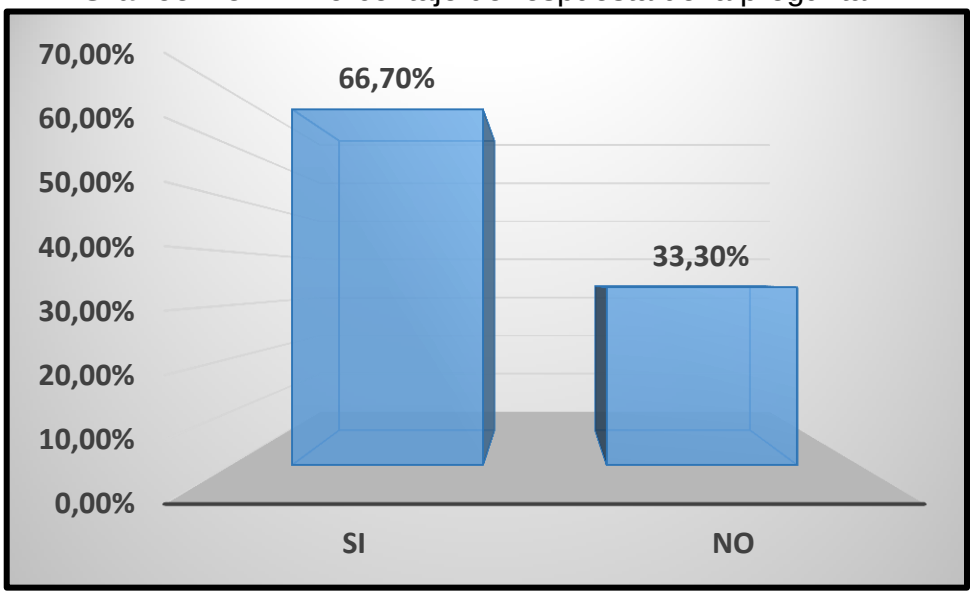
4. ¿Considera usted que con el miniordenador Raspberry PI Zero W los riesgos se podrán mantener controlados?

Tabla No. 9 Respuesta de la pregunta 4

Alternativas	Cantidad	Porcentajes
SI	10	66.7%
NO	5	33.3%
Total	15	100.0%

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 14 Porcentaje de respuesta de la pregunta 4



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Análisis: Durante la encuesta realizada se verifico que el 66.7% de los usuarios consideran que el miniordenador Raspberry PI Zero aplicara técnicas para mantener los riesgos controlados.

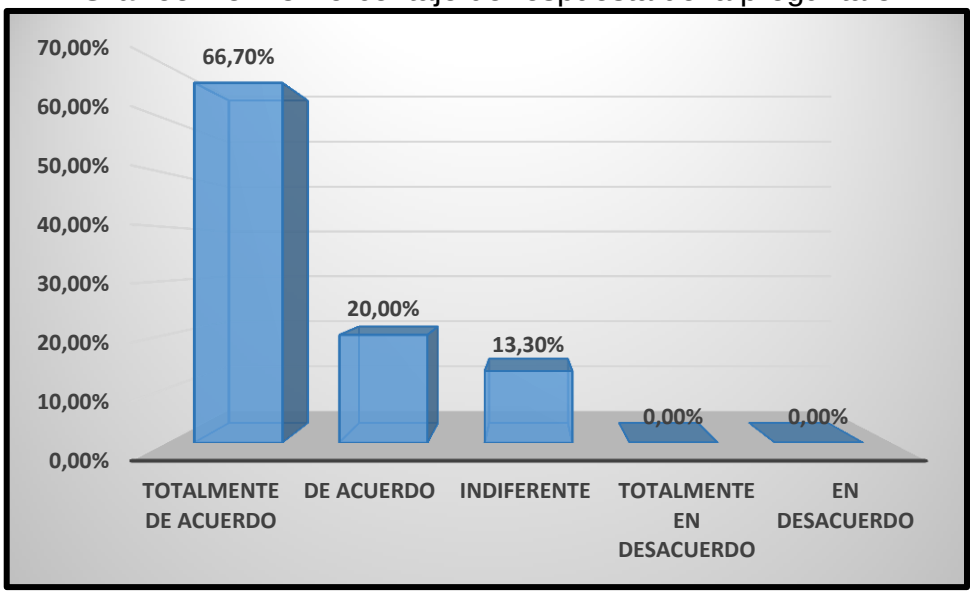
5. ¿Está usted de acuerdo que se implemente una guía de buenas prácticas para los usuarios y administradores de red sobre el buen uso del internet y el manejo de los puertos y conectores de los ordenadores?

Tabla No. 10 Respuesta de la pregunta 5

Alternativas	Cantidad	Porcentajes
Totalmente de acuerdo	10	66.7%
De acuerdo	3	20.0%
Indiferente	2	13.3%
Totalmente en desacuerdo	0	0.0%
En desacuerdo	0	0.0%
Total	15	100.0%

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 15 Porcentaje de respuesta de la pregunta 5



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Análisis: Durante la encuesta realizada se verifico que el 66.7% de los usuarios están totalmente de acuerdo que se implemente una guía de buenas prácticas para obtener conocimientos sobre el uso de los navegadores de internet y los puertos y conectores de los ordenadores.

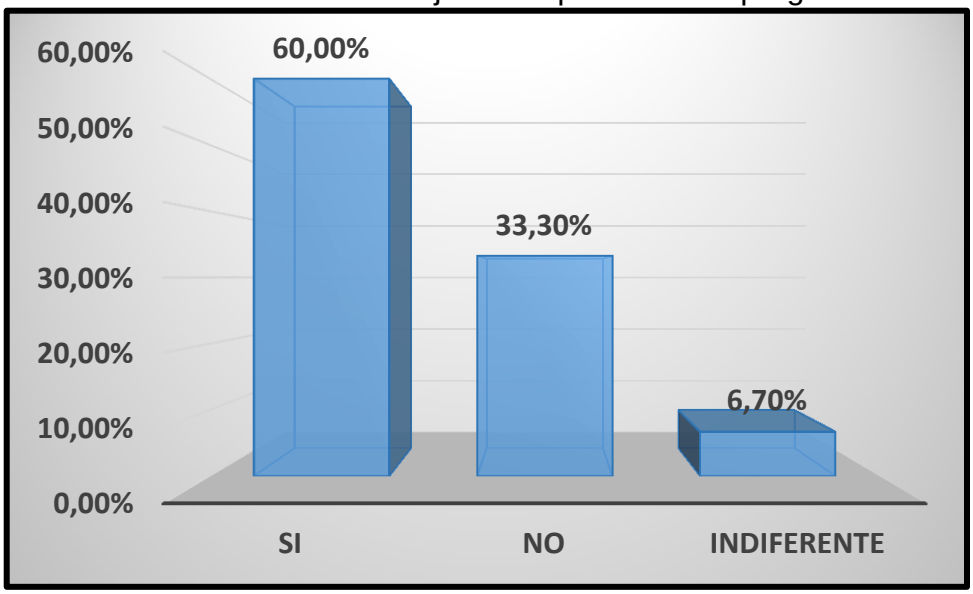
6. Considera usted importante la implementación de métodos de protección en los ordenadores como: ¿bloqueo de puertos USB inutilizables, ejecución de antivirus licenciado y demás?

Tabla No. 11 Respuesta de la pregunta 6

Alternativas	Cantidad	Porcentajes
SI	9	60.0%
NO	5	33.3%
Indiferente	1	6.7%
Total	15	100.0%

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 16 Porcentaje de respuesta de la pregunta 6



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Análisis: Durante la encuesta realizada se verifico que el 60.0% de los usuarios consideran que es de vital importancia la aplicación de métodos de seguridad como: bloqueo de puertos USB inutilizables e implementación de antivirus licenciados.

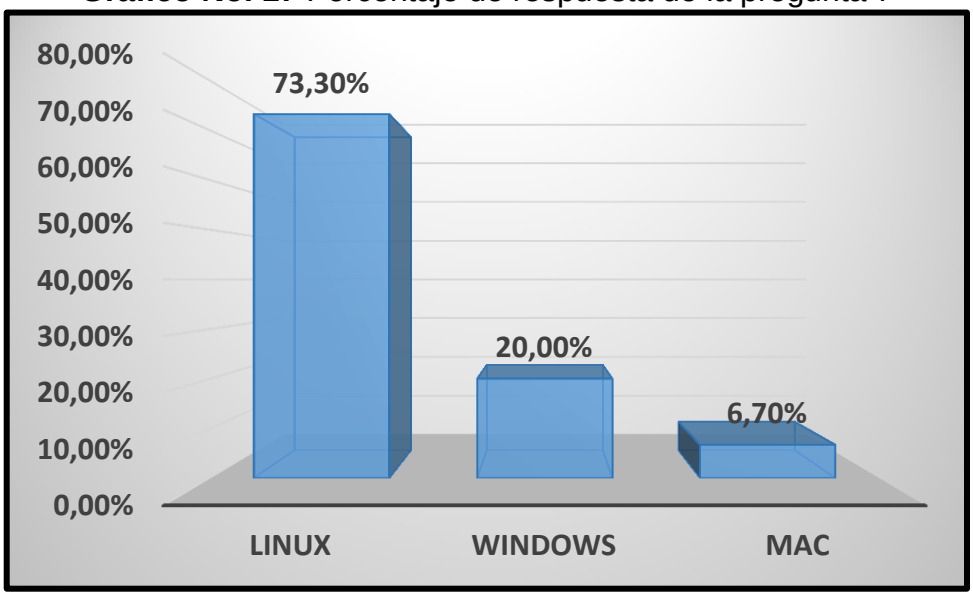
7. ¿Qué sistema operativo tiene instalado en sus ordenadores?

Tabla No. 12 Respuesta de la pregunta 7

Alternativas	Cantidad	Porcentajes
Linux	11	73.3%
Windows	3	20.0%
MAC	1	6.7%
Total	15	100.0%

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 17 Porcentaje de respuesta de la pregunta 7



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Análisis: Durante la encuesta realizada se verifico que el 73.3% de los usuarios utilizan Ubuntu como sistema operativo en sus ordenadores.

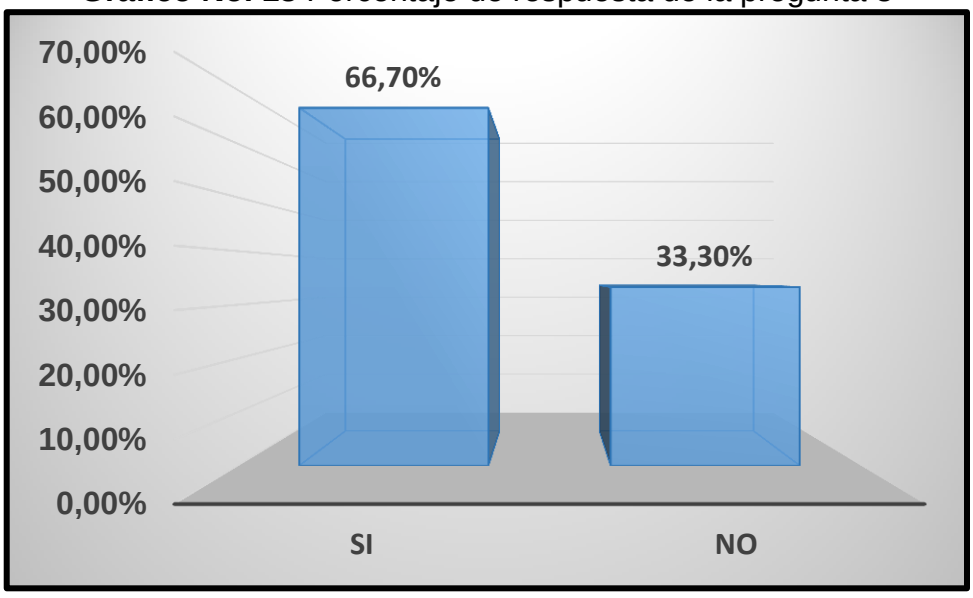
8. ¿Considera usted establecer un reporte de vulnerabilidades que pueden ser explotadas por el miniordenador Raspberry PI Zero para ejecutar el respectivo tratamiento de esta disminuyendo los riesgos?

Tabla No. 13 Respuesta de la pregunta 8

Alternativas	Cantidad	Porcentajes
SI	10	66.7%
NO	5	33.3%
Total	15	100.0%

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 18 Porcentaje de respuesta de la pregunta 8



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Análisis: Durante la encuesta realizada se verifico que el 66.7% de los usuarios consideran que importante establecer un reporte de vulnerabilidades que pueden ser explotadas por la placa Raspberry PI Zero para ejecutar su respectivo tratamiento minimizando los riesgos presentes.

3.1.6 VALIDACIÓN DE LA HIPÓTESIS

Los resultados que fueron proporcionados a través de las encuestas a los usuarios otorgan sustentación al desarrollo del proyecto, en base a una muestra de 15 personas que fue seleccionada con el objetivo de conseguir transparencia y un gran nivel de aceptabilidad de la propuesta tecnológica donde se verifique la validez de los datos. Conocer los requerimientos, necesidades ayuda a contribuir con una planificación de forma específica de estudio para aclarar dudas o corregir posibles errores inconsistentes que solo los usuarios operacionales pueden conocer y que podrían presentarse durante un proceso de recopilación de información o en tal caso durante la ejecución de ambientes de pruebas o escenarios controlados aplicando miniordenadores como el Raspberry PI Zero W que forma parte del proyecto.

Una vez culminado con todos los procesos de recolección de datos aplicando la técnica de instrumento la encuesta, se realiza la creación de los documentos que almacenen toda la información detallada por los encuestados, validando como fundamento principal la implementación del proyecto en beneficio de la empresa PYME “Marcelo Rúales”.

4. CAPÍTULO IV

4.1 PROPUESTA TECNOLÓGICA

4.1.1 ANÁLISIS DE FACTIBILIDAD

Una vez planteado el problema en la empresa Marcelo Rúales sobre las posibles vulnerabilidades presentes en la infraestructura de red de área local se evidencio la necesidad de poder ejecutar un análisis de vulnerabilidades utilizando la placa electrónica Raspberry PI W - PT, con la finalidad de detectar los riesgos que conllevan a la sustracción de datos sensibles de la pequeña compañía donde se está desarrollando el proyecto, en lo cual atacantes pueden conectar pequeños dispositivos en los ordenadores para establecer un ataque cibernético y tener el acceso a la confidencialidad de la información beneficiándose económicamente. A continuación, se detallará las factibilidades operacionales, técnicas, económicas y legales para identificar el nivel de aceptación de la propuesta tecnológica.

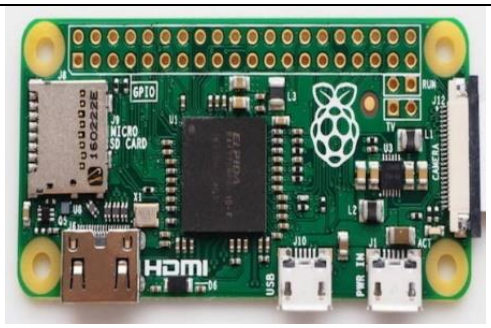
4.1.2 FACTIBILIDAD OPERACIONAL

Uno de los objetivos de analizar la factibilidad operacional del proyecto es la de investigar si la placa electrónica Raspberry PI W - PT sugerida para realizar un análisis de vulnerabilidades será utilizada por la pequeña empresa Marcelo Rúales. El proyecto referente al análisis de vulnerabilidades se lo denomina operativo, por lo cual este tipo de análisis evaluará los ordenadores, Laptops, servidores y demás que se conectan a una red por medio de su interfaz USB (Universal Serial Bus), haciendo uso de una simulación de ataque físico y de esta forma poder identificar los posibles fallos de seguridad que posee las estaciones de trabajo conectadas a una red de área local con acceso a internet o a una red inalámbrica para finalmente poder disminuir los riesgos que producen perdidas de información confidencial ocasionando daños en la productividad del negocio.

4.1.3 FACTIBILIDAD TÉCNICA

En esta factibilidad se detallará los componentes de hardware y software que serán utilizados en el desarrollo de la implementación del proyecto.

Tabla No. 14 Factibilidad técnica

Hardware	Características
	• Procesador CORE I5. • Sistema operativo Windows 10 de 64 Bits. • 6 gigabytes de memoria RAM.
	• Inyección de puertas traseras. • Conversión de la interfaz USB en ETHERNET • Captura de tráfico desde la red de internet.
	• Procesador CORE I7. • Sistema operativo Windows 10 de 64 bits. • 16 gigabytes de memoria RAM.
Software	**Características**
	• Sistema operativo Windows 10 de 64 bits.

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

4.1.4 FACTIBILIDAD ECONÓMICA

En esta etapa se detallará los gastos que se generan en el desarrollo del proyecto referente al análisis de vulnerabilidades utilizando la placa electrónica Raspberry PI POISONTAP.

Tabla No. 15 Costos del proyecto

Descripción	Costo unitario
Servicio de Internet	$ 30
Laptop CORE I5	$ 500
Laptop CORE I7	$ 700
Raspberry PI POISONTAP	$ 45
Otros Gastos	$ 100
Costo Total	$ 1375

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

4.1.5 FACTIBILIDAD LEGAL

El análisis de vulnerabilidades aplicando la herramienta PT no vulnera ni viola el Código Orgánico Integral Penal vigente y establecido en la República del Ecuador ya que solo se ejecutará un escenario de prueba para diagnosticar los posibles fallos de seguridad en la empresa Marcelo Rúales ubicada en la ciudad de Guayaquil.

4.1.6 ETAPAS DE METODOLOGÍA DEL PROYECTO

Para el desarrollo del proyecto de titulación se aplicaron los procesos de la metodología Scrum en lo cual la misma se la utiliza para poder llevar a cabo la ejecución de la propuesta tecnológica siguiendo los lineamientos de forma clasificada y empleando secuencia del proyecto por medio de fases, con el objetivo de obtener los resultados finales de las pruebas de Hackeo ético a través de la placa Raspberry PI Zero W.

En el proyecto se lo ha implementado empleando un conjunto de elementos que forman parte de una lista de actividades que integra la metodología Scrum en lo cual fueron seleccionadas para conformar el objetivo Sprint.

Los objetivos Sprint son los siguientes

- En este proyecto se indica que elementos de la lista de actividades se aplicaran.

- El auditor de seguridad informática cuenta con un tipo de dos meses para ejecutar las fases de Hackeo ético por medio de una placa electrónica llamada Raspberry PI Zero W.

- El auditor de seguridad informática ejecutas las fases de reconocimiento, escaneo, obtención del acceso, mantenimiento del acceso y borrado de huellas por medio de la placa Raspberry PI Zero W con el objetivo de determinar las amenazas y vulnerabilidades de la red de área local.

Fases de planificación de la metodología Scrum

- **Etapa I:** Configuración e instalación del sistema operativo en la placa Raspberry PI Zero**.**

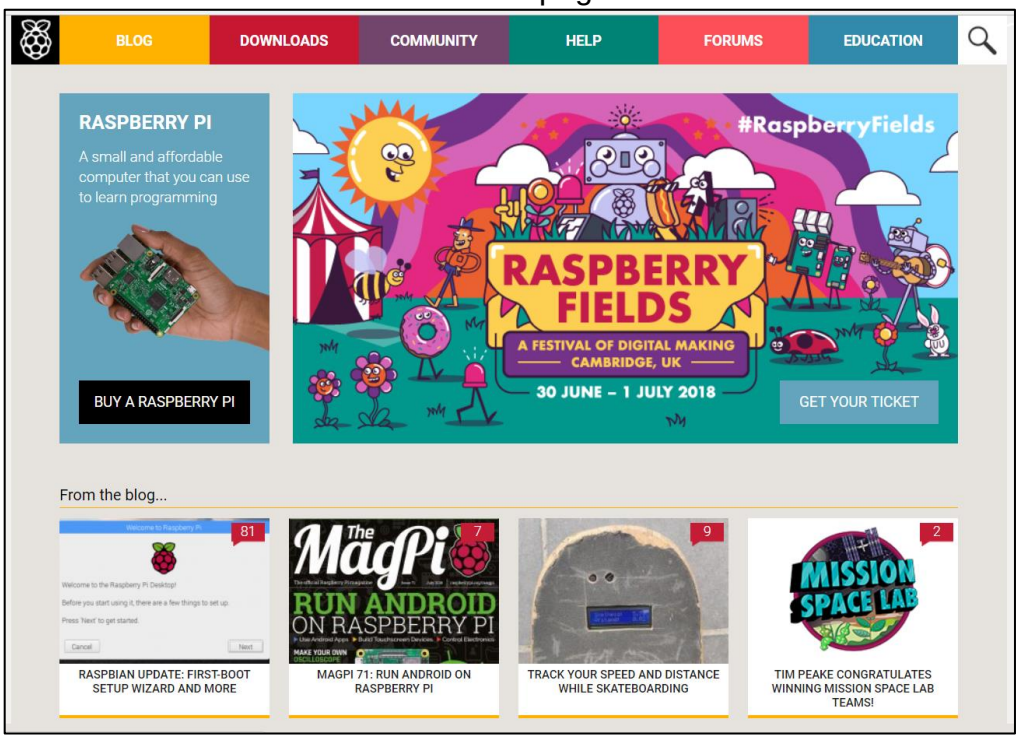
- **Etapa II:** Instalación de los paquetes de PT por medio de la página de GitHub.
- **Etapa III:** Configuración del Archivo de PT para efectuar el ataque.

- **Etapa IV:** Ejecución del ataque informático y verificación de la conexión con el cliente víctima.

Etapa I: Instalación del sistema operativo Raspbian en el miniordenador RASPEBRRY PI ZERO W.

Antes de iniciar la instalación del Raspbian se procede a acceder a la página www.raspberrypi.org para la descarga del sistema operativo como se ve en el gráfico No. 19.

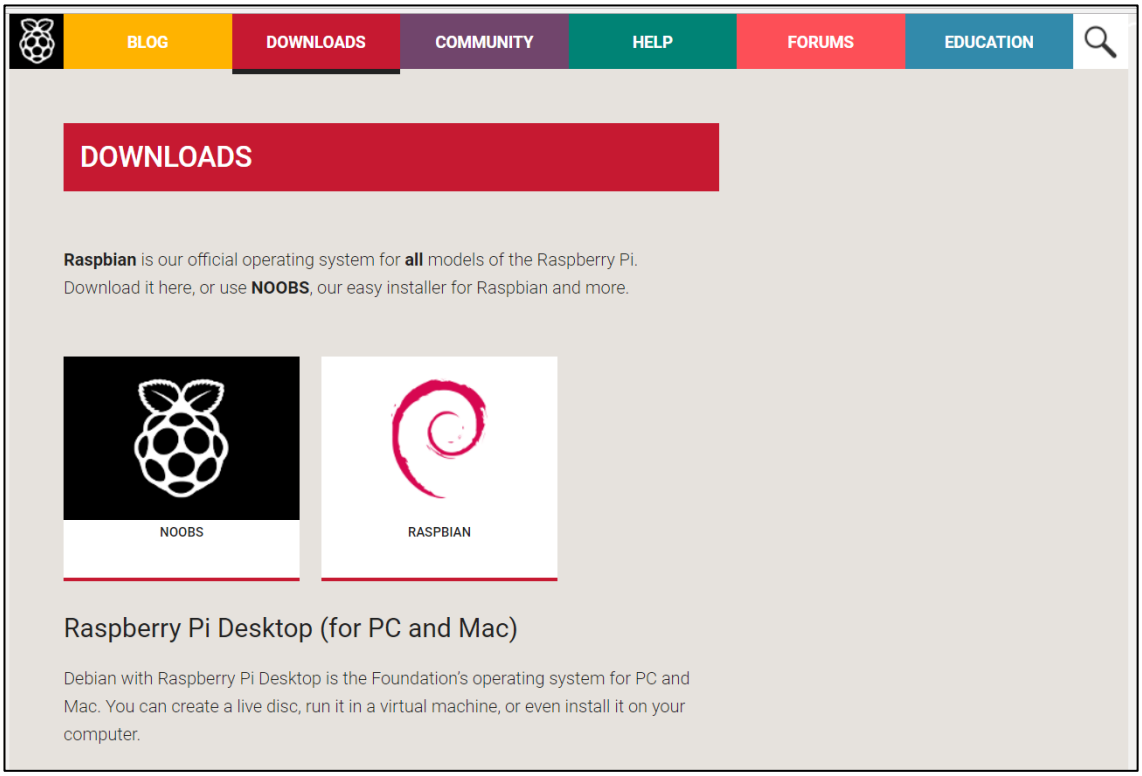
Gráfico No. 19 Acceso a la página RASPBERRY PI



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

En este caso se procede a seleccionar el sistema para iniciar con la instalación de este en la placa electrónica Raspberry PI Zero. En esta parte se escoge la opción Noobs como se ve el gráfico No. 20.

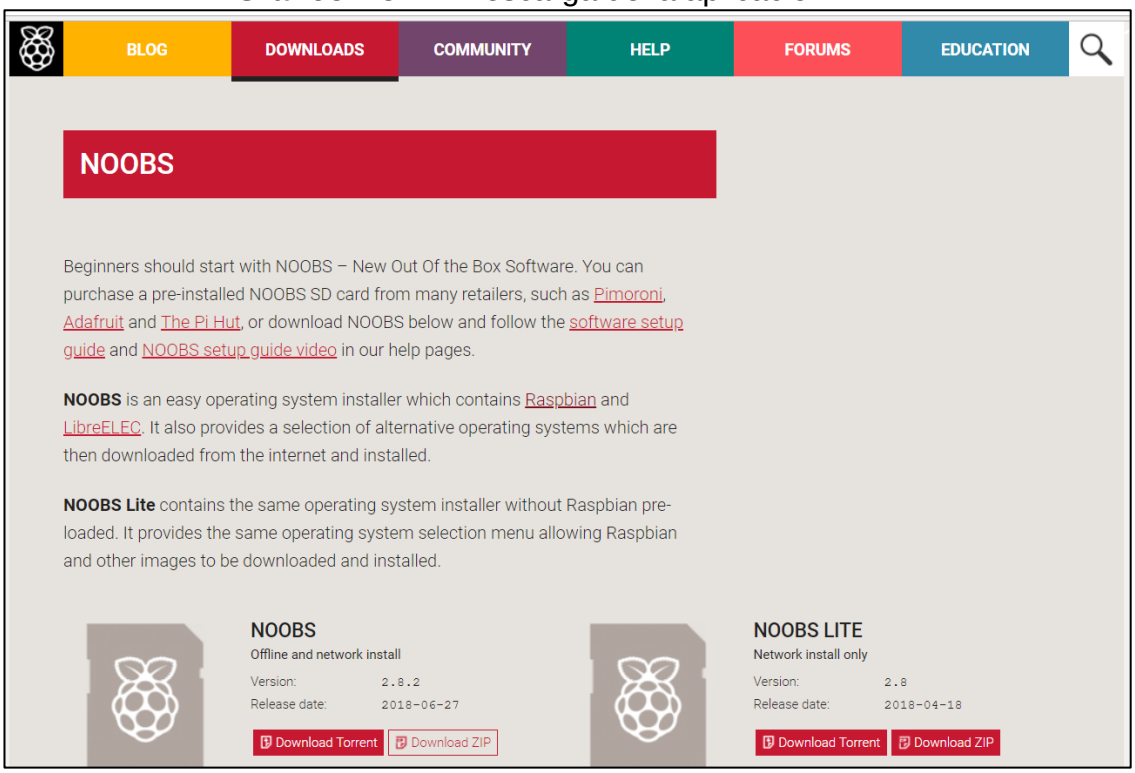
Gráfico No. 20 Selección del sistema a instalar



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Una vez seleccionado el sistema operativo se procede con la descarga de este en formato ZIP como se ve en el gráfico No. 21.

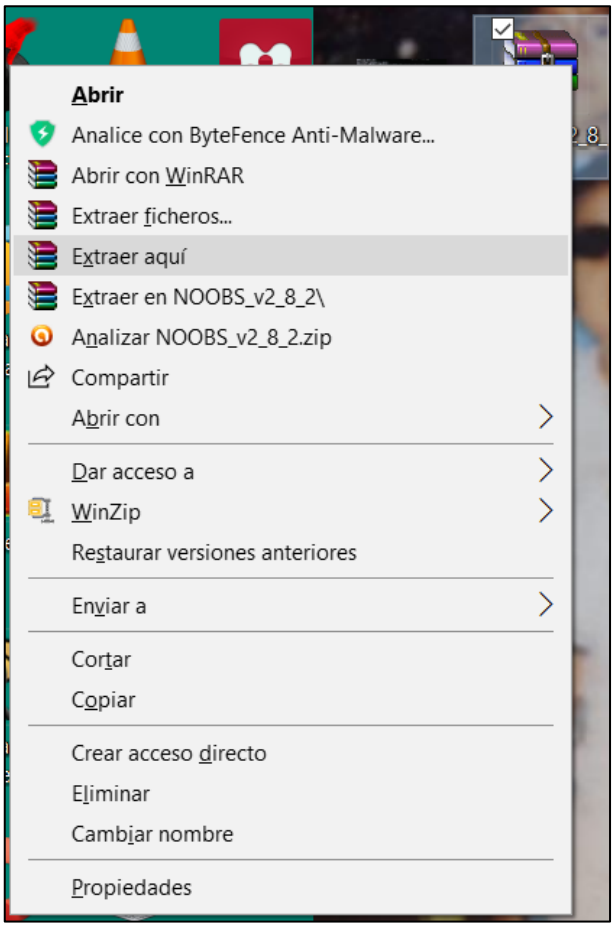
Gráfico No. 21 Descarga de la aplicación



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Después de haber procedido con la descarga del sistema operativo se da inicio con la extracción de los archivos para después pasarlos a la tarjeta de memoria como se ve en el gráfico No. 22.

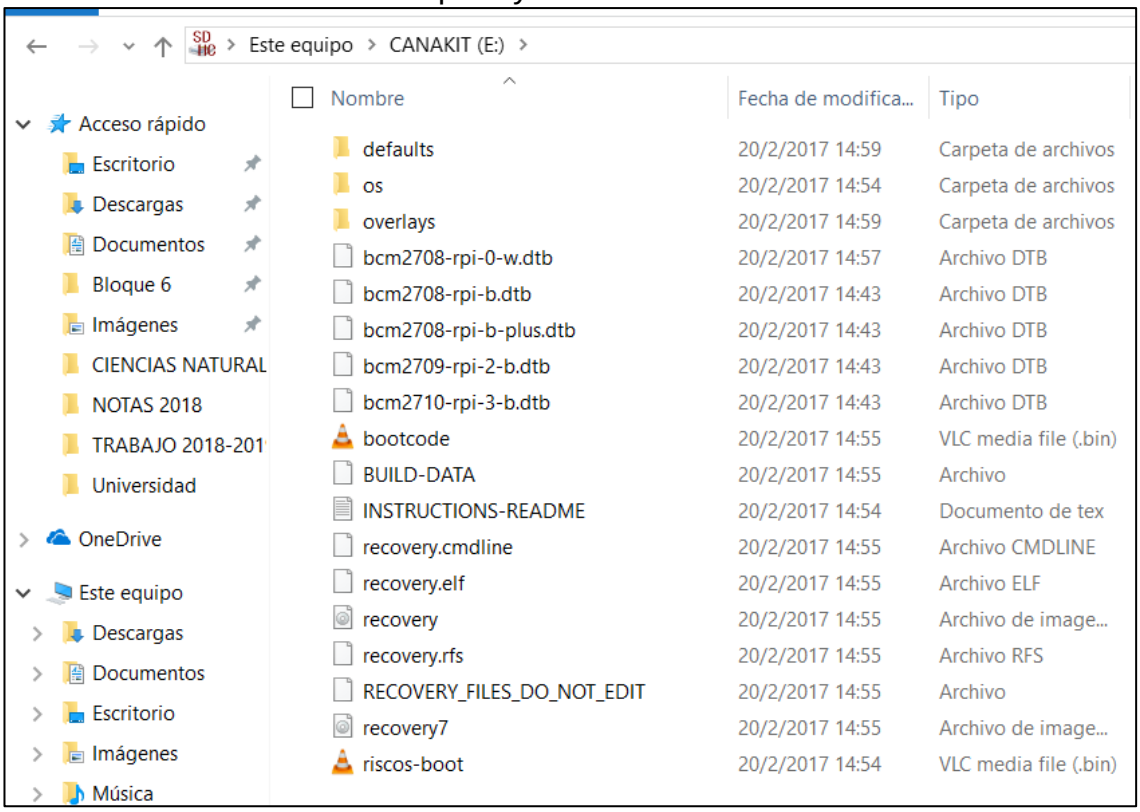
Gráfico No. 22 Extracción de los archivos



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Una vez cumplido con el proceso de extracción del archivo .ZIP se procede con la copia de estos a la tarjeta de memoria de Raspberry PI como se ve en el gráfico No. 23.

Gráfico No. 23 Proceso de copia de los archivos a la memoria de Raspberry Pi Zero W



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

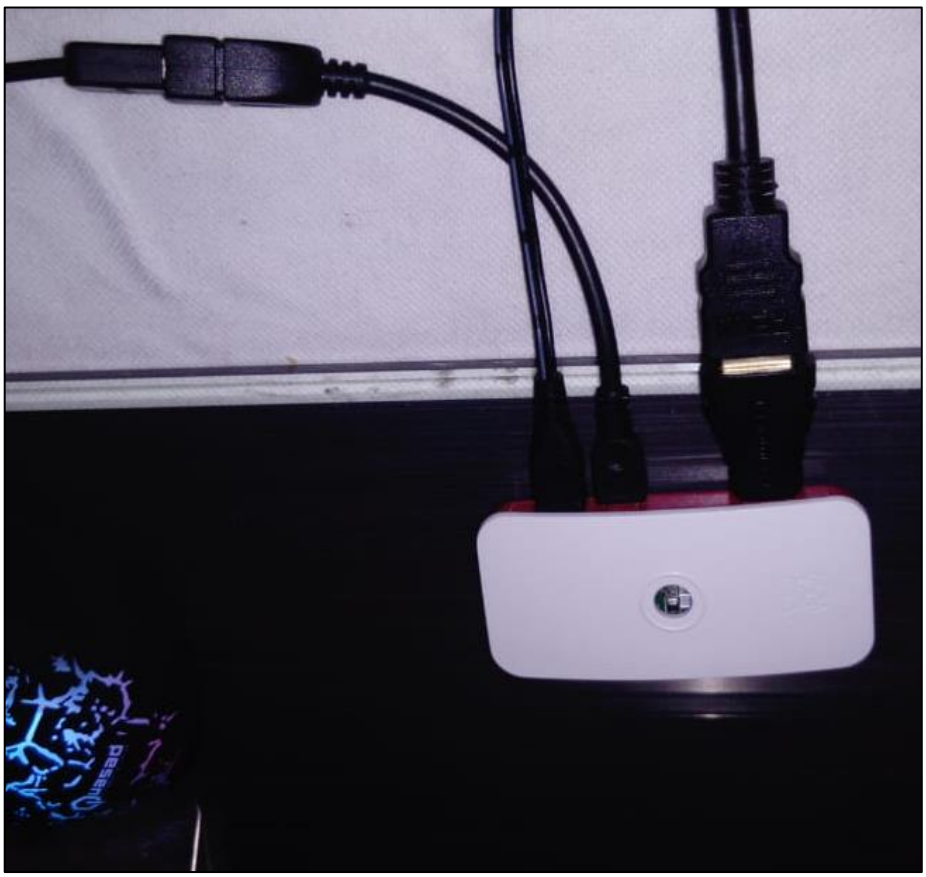
Una vez descargado el sistema operativo NOOBS se procede a integrar el miniordenador RASPBERRY PI ZERO W con la carcasa como se ve en el gráfico No. 23.

Gráfico No. 24 Instalación de la carcasa en el mini ordenador

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

En esta sección de la implementación del miniordenador se procede a conectar los cables USB y HDMI en la placa electrónica como se ve en el gráfico No. 25.

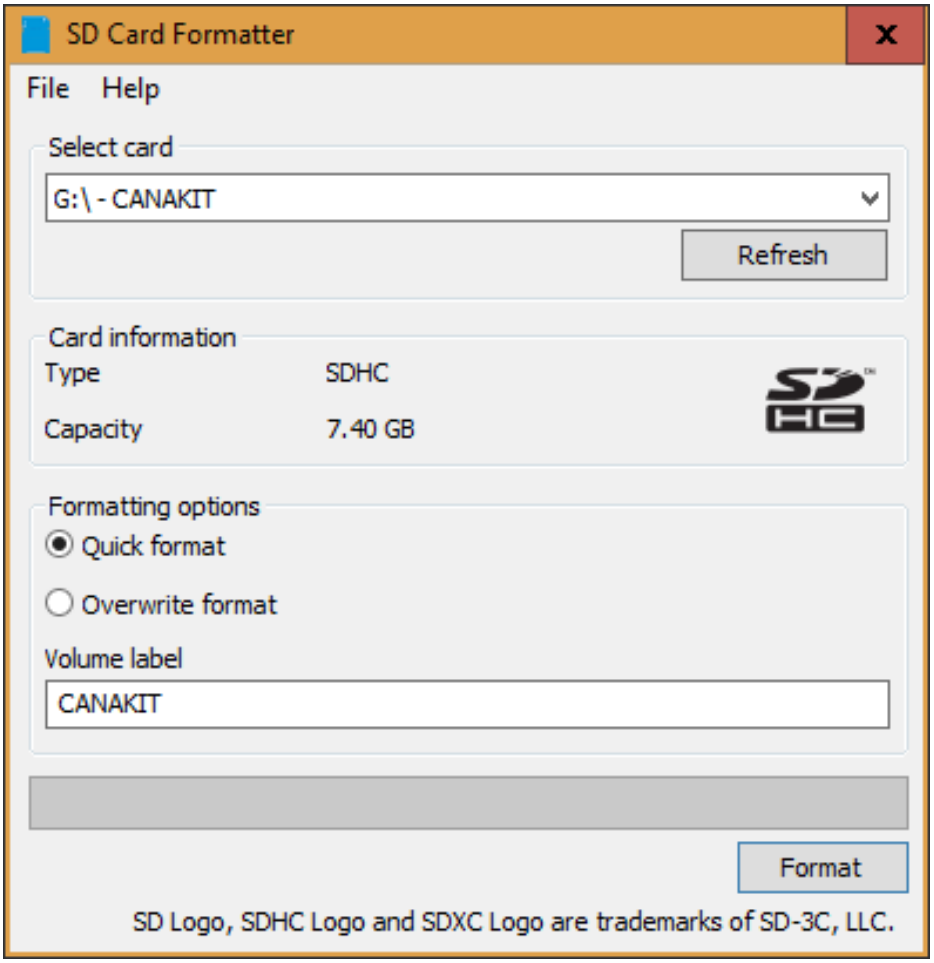
Gráfico No. 25 Conexión de los cables con la placa RASPBERRY PI ZERO



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Antes de instalar el sistema operativo NOOBS en el mini CPU RASPBERRY PI ZERO W, se procede con el formateo de la tarjeta de memoria como se ve en el gráfico No. 26.

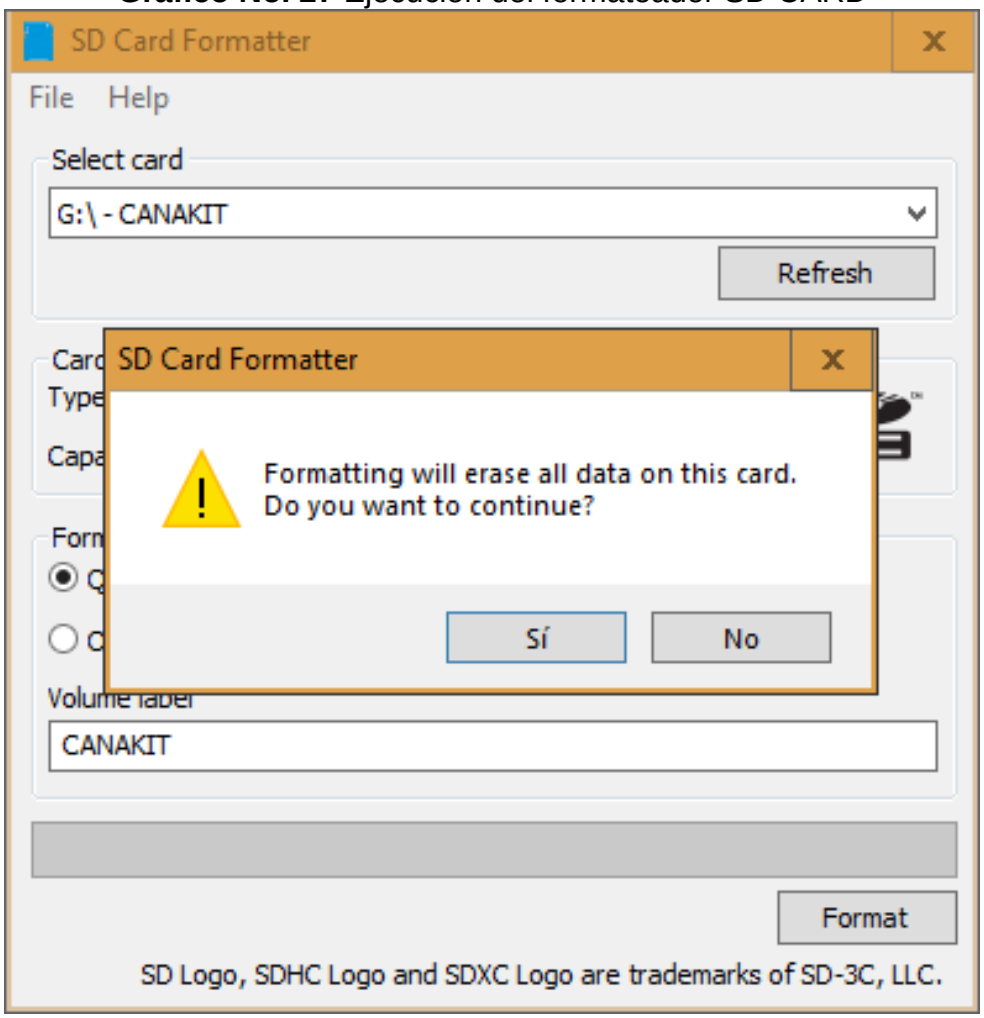
Gráfico No. 26 Inicio de la herramienta SD CARD Formatter



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Después de haber integrado la tarjeta de memoria con el lector en la computadora se inicia con la herramienta formateadora y se da clic en formato y aparece un mensaje de confirmación como se ve en el gráfico No. 27.

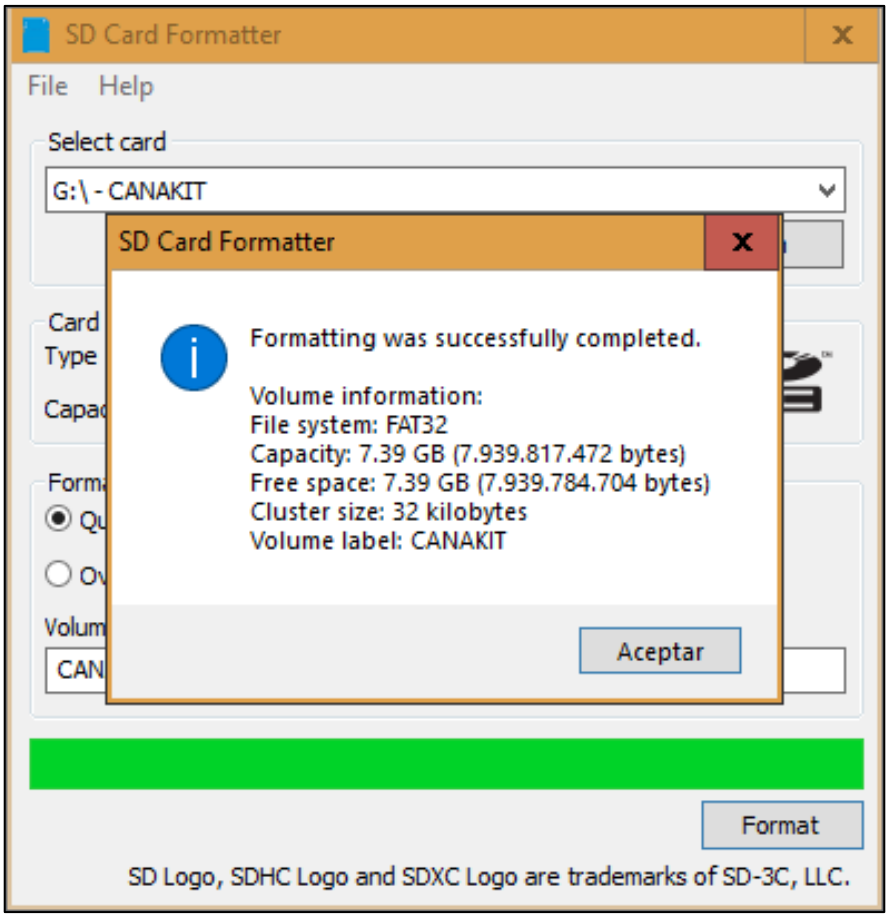
Gráfico No. 27 Ejecución del formateador SD CARD



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

En este mensaje de confirmación se le da clic en SI y se empieza a formatear la tarjeta de memoria del RASPBERRY PI ZERO W como se ve en el gráfico No. 28.

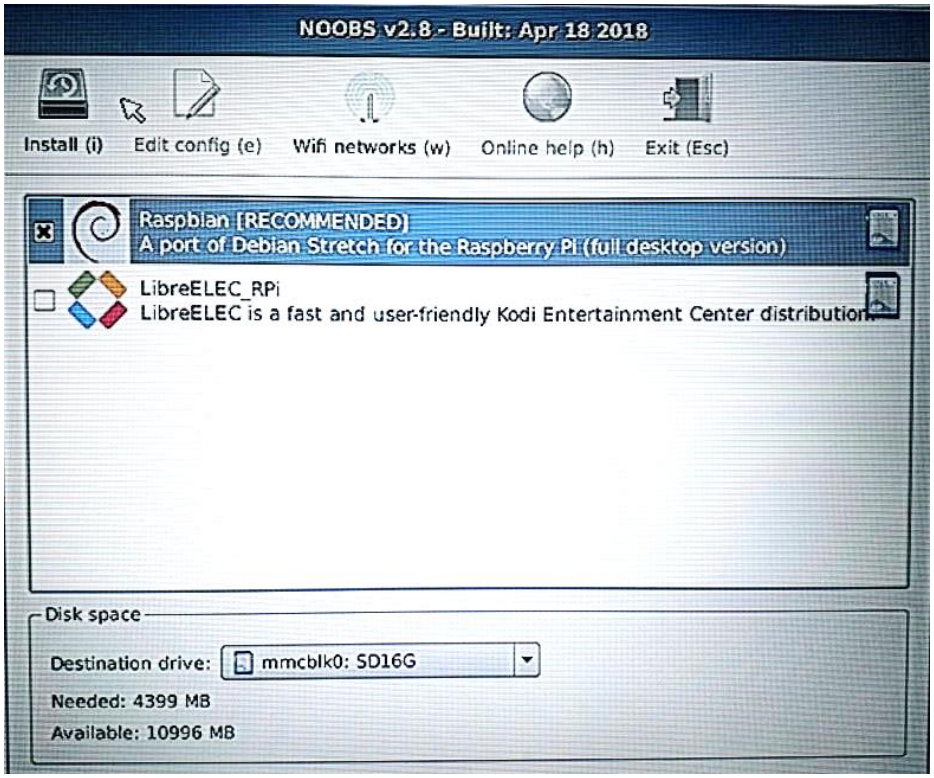
Gráfico No. 28 Formateo terminado



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Una vez efectuado el proceso de formateo de memoria se procede a seleccionar el tipo de sistema a instalar en este caso se elige NOOBS como se ve en el gráfico No. 29.

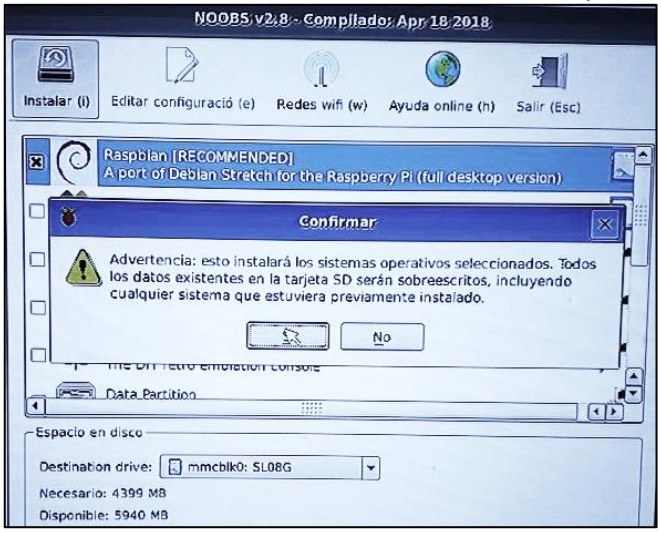
Gráfico No. 29 Selección del sistema a instalar



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Una vez seleccionado el sistema operativo a instalar le damos clic en SI y se procede con la instalación antes del proceso elegimos el tipo de teclado como se ve en el gráfico No. 30.

Gráfico No. 30 Confirmación del Sistema Operativo



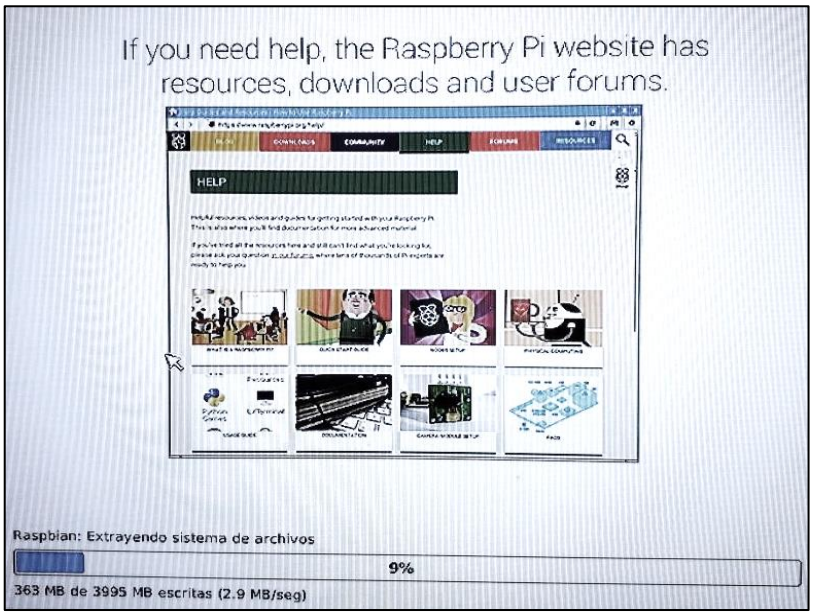
Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 31 Selección del tipo de teclado

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Después del mensaje de confirmación se cargan los repositorios de la instalación como se ve en el gráfico No. 32.

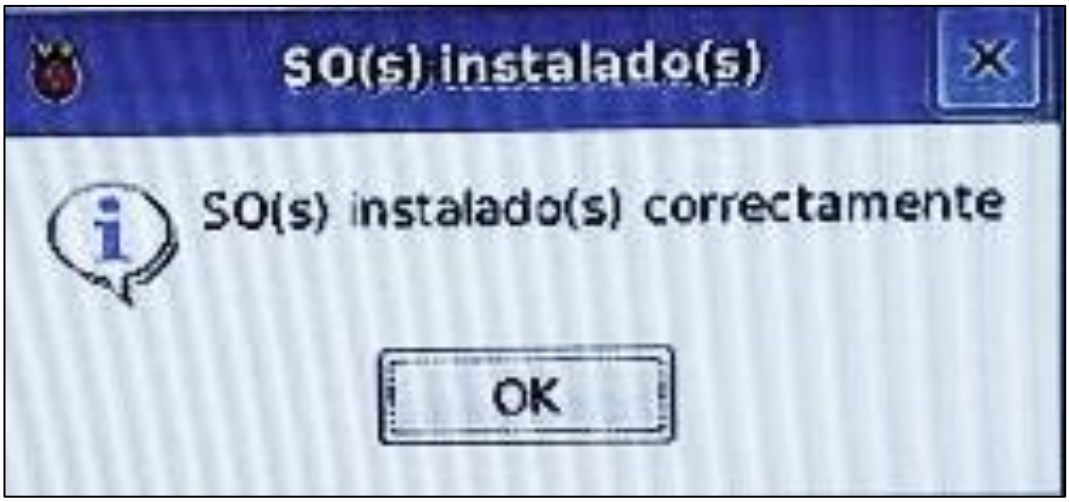
Gráfico No. 32 Proceso de instalación



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Después de haberse cargado los repositorios se finaliza la instalación del sistema operativo NOOBS en el RASPBERRY PI ZERO W como se ve en el gráfico No. 33.

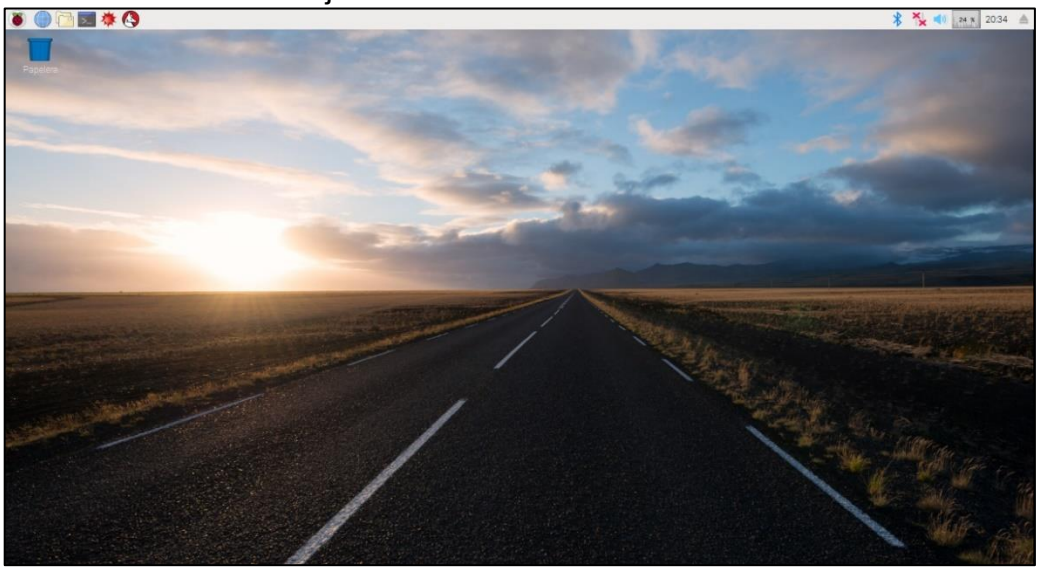
Gráfico No. 33 Proceso de instalación finalizado



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Una vez culminada con la instalación del sistema operativo NOOBS se procede a la carga del sistema operativo como se ve en el gráfico No. 34.

Gráfico No. 34 Mensaje de confirmación de finalización de la instalación

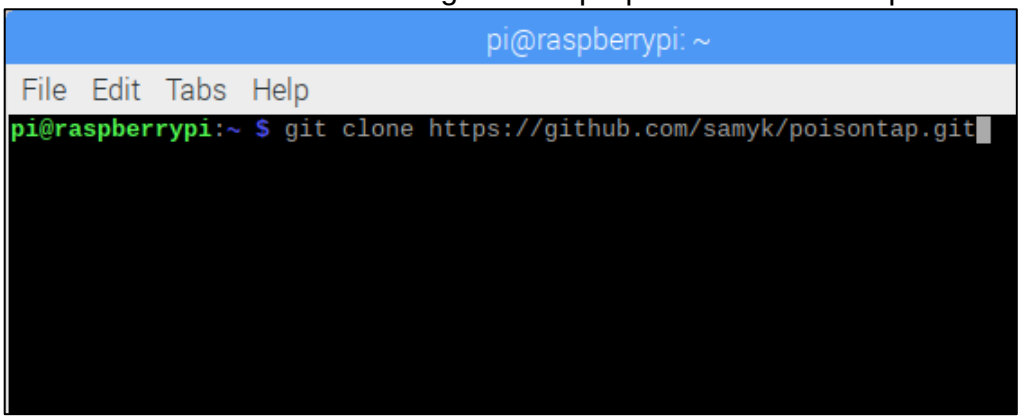


Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

- **Etapa II:** Instalación y configuración de los paquetes de Poisontap en el sistema operativo NOOBS.

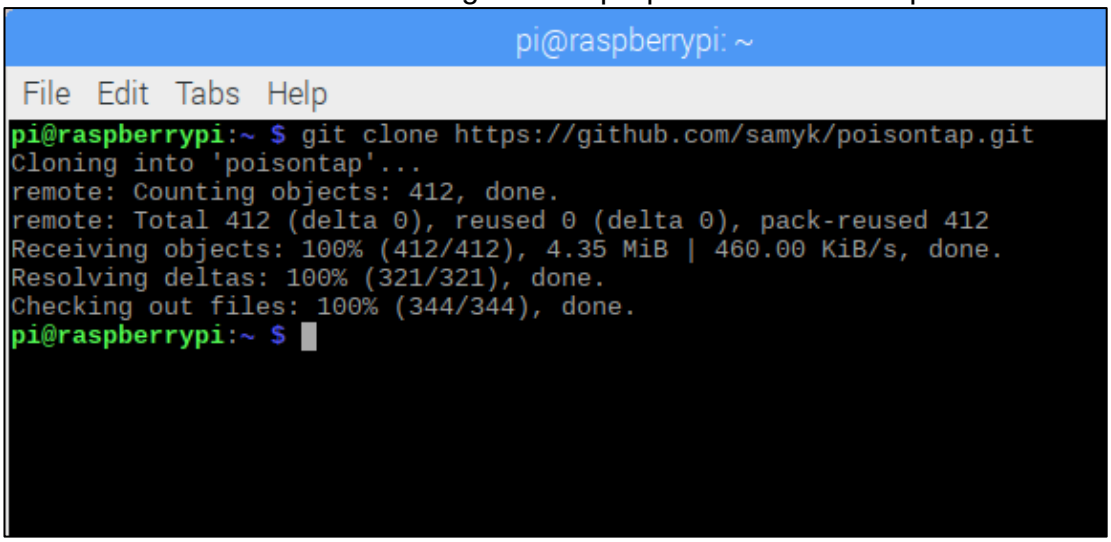
Después de la instalación del sistema operativo NOOBS se procede con la descarga de los paquetes desde la página de github.com como se ve en el gráfico No. 35 y No. 36.

Gráfico No. 35 Descarga de los paquetes de Poisontap



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

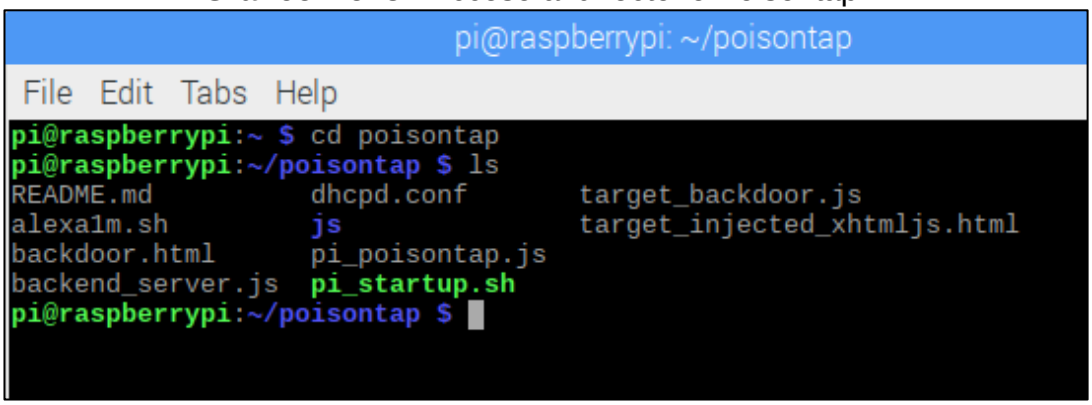
Gráfico No. 36 Descarga de los paquetes de Poisontap



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Después de haber descargado los paquetes se procede a acceder al directorio Poisontap como se ve en el gráfico No. 37.

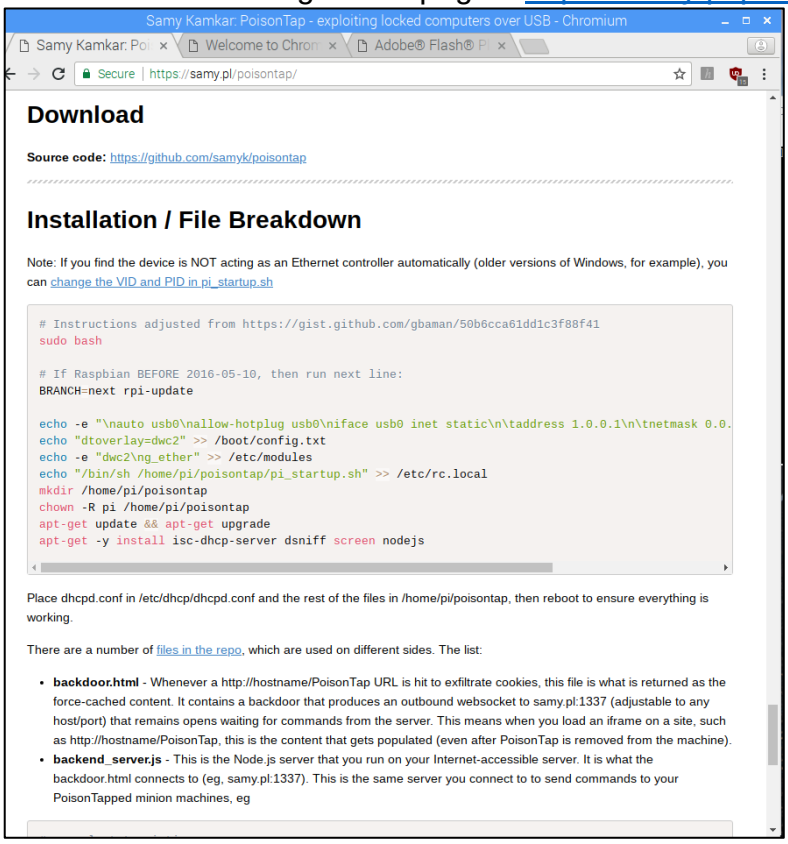
Gráfico No. 37 Acceso al directorio Poisontap



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Una vez accedido al directorio Poisontap se procede a configurar el archivo install.sh, y se pega el siguiente código que se encuentra en la página https://samy.pl/poisontap/ como se ve en el gráfico No. 38.

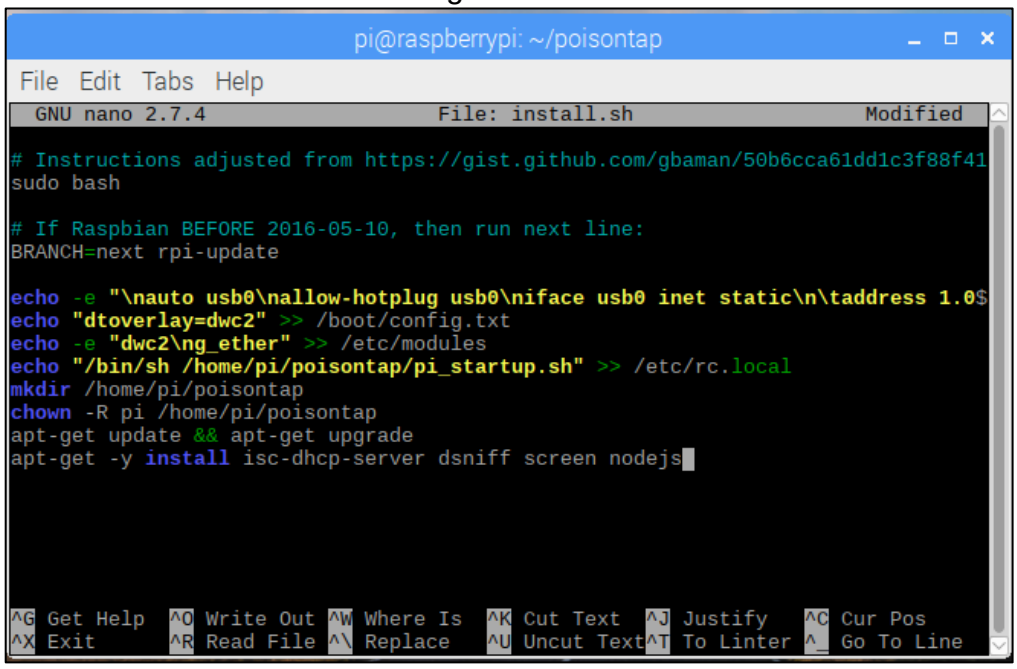
Gráfico No. 38 Acceso al código en la página https://samy.pl/poisontap/



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

En esta ventana se pega el código en el archivo install.sh. Como se ve en el gráfico No. 39.

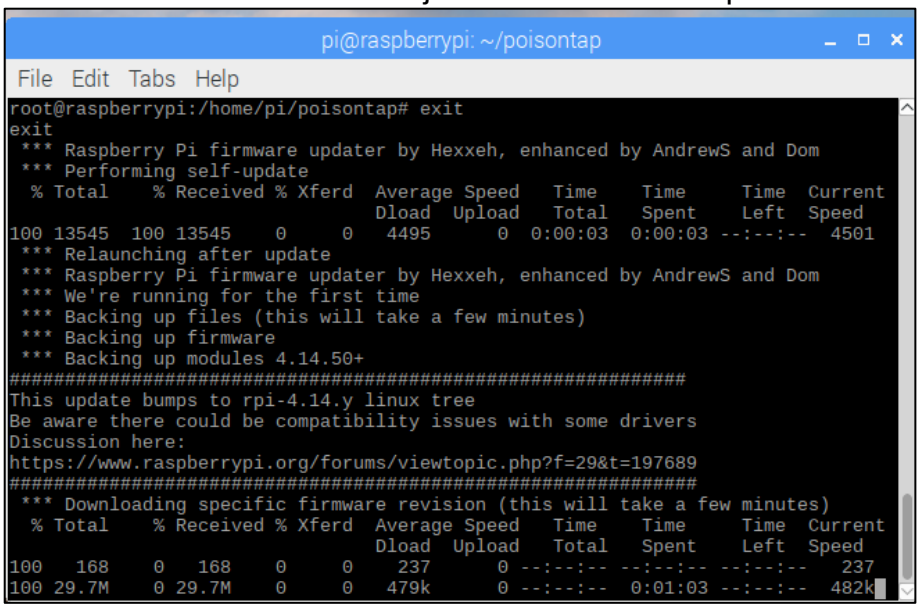
Gráfico No. 39 configuración del archivo install.sh



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Después de haber configurado el archivo install.sh se procede a ejecutar el Poisontap como se ve en el gráfico No. 40.

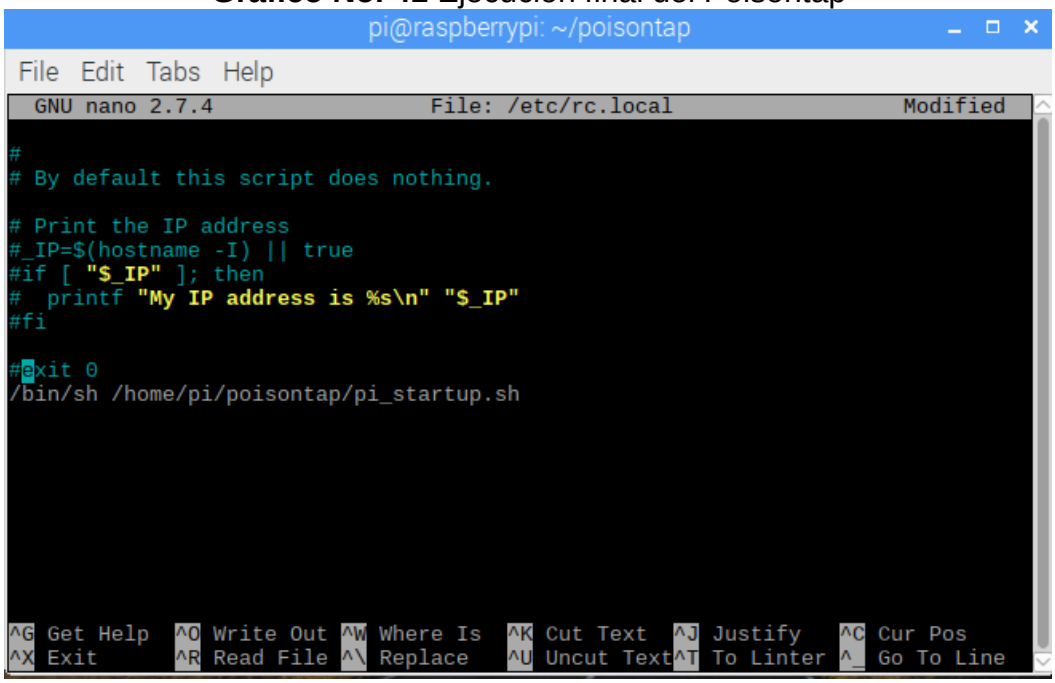
Gráfico No. 40 Ejecución del Poisontap



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Después de haber configurado el Poisontap se elimina las líneas de códigos del archivo rc.local que se encuentra ubicado en el directorio etc. Como se ve en el gráfico No. 41.

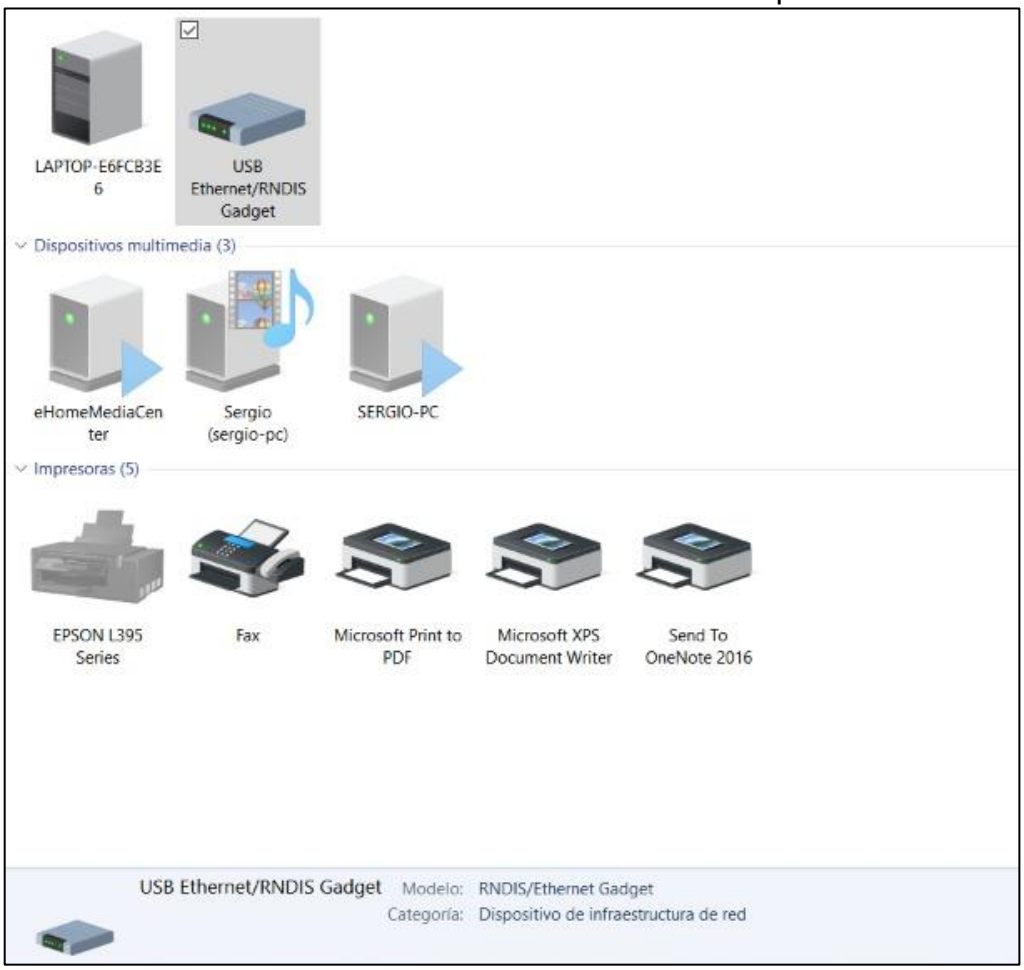
Gráfico No. 41 Ejecución final del Poisontap



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

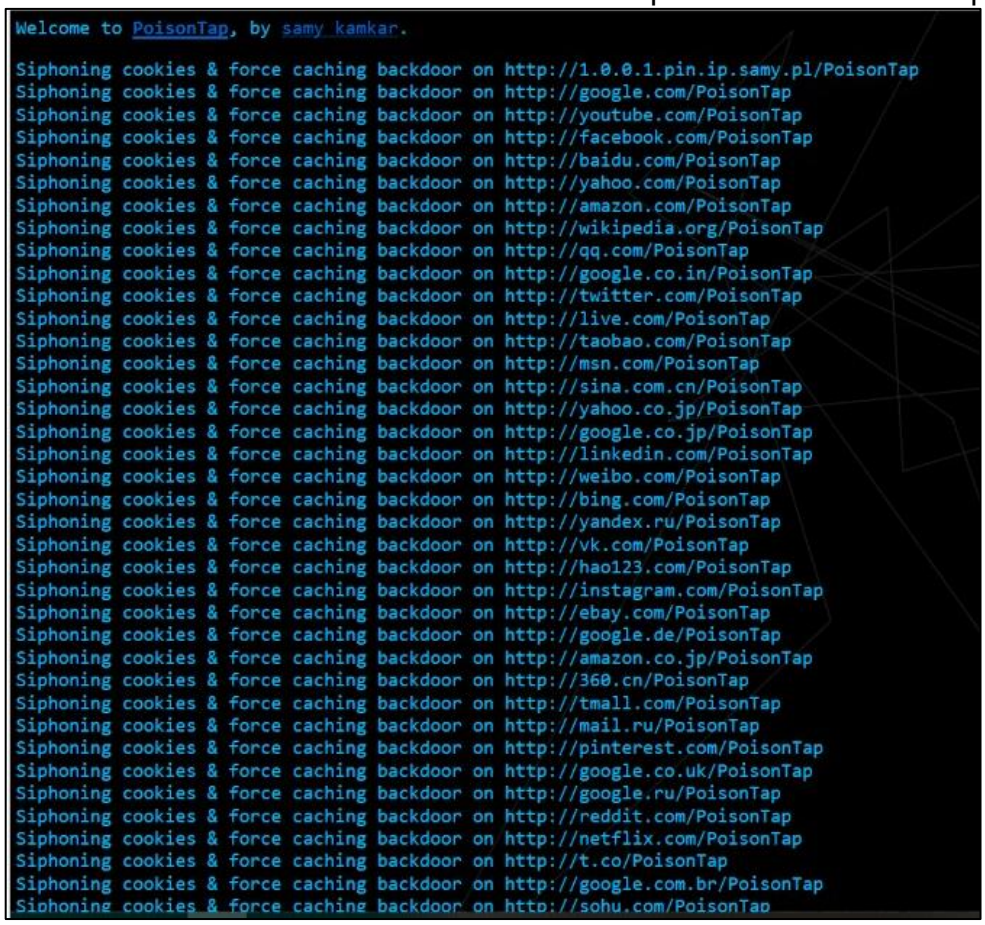
Una vez configurado el Raspberry PI Zero W - PT se lo conecta a un ordenador vía puerto USB (Universal Serial Bus) para el reconocimiento de la placa en modo Ethernet. Además, para verificar la información por medio de Poisontap se procede a digitar la dirección IP 1.0.0.1 en el navegador web del ordenador como se ve en el gráfico No. 42 y 43.

Gráfico No. 42 Conexión del Poisontap



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

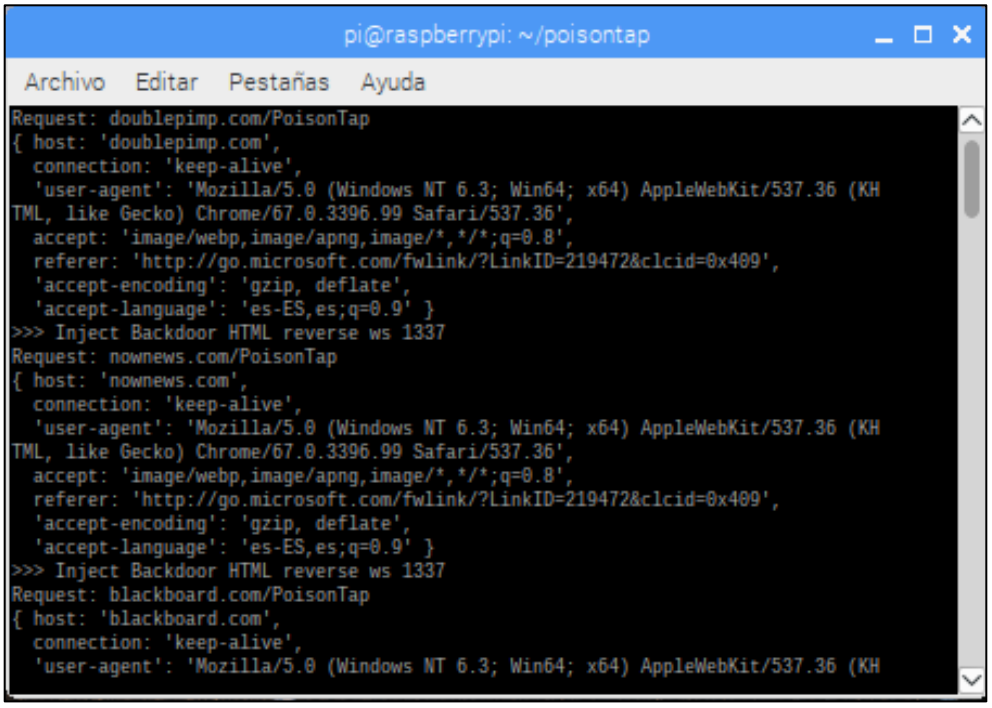
Gráfico No. 43 Verificación de la información por medio de Poisontap



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

En este caso se procede a acceder al archivo de POISONTAP con extensión LOG, después de haberse conectado con el servidor víctima como se ve en el gráfico No. 44.

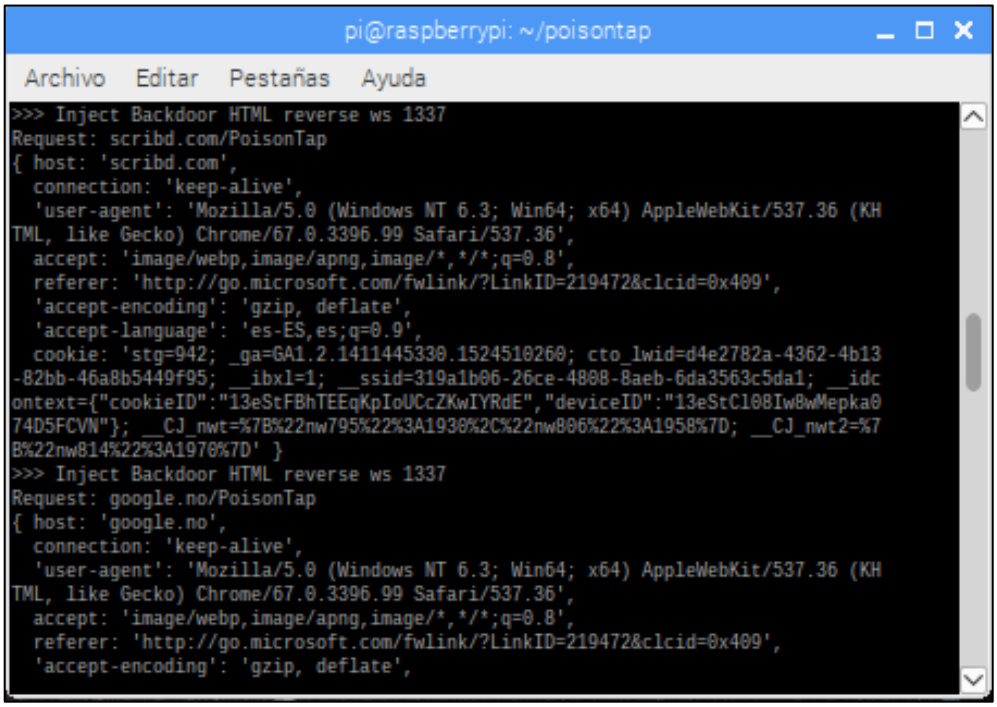
Gráfico No. 44 Acceso al archivo con extensión LOG



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

En este caso se verifica el archivo LOG y se comprueba el tipo de Backdoor inyectado, además se verifica la versión del sistema operativo Microsoft y el tipo de red que se conectó él dispositivo cliente, como se ve en el gráfico No. 45.

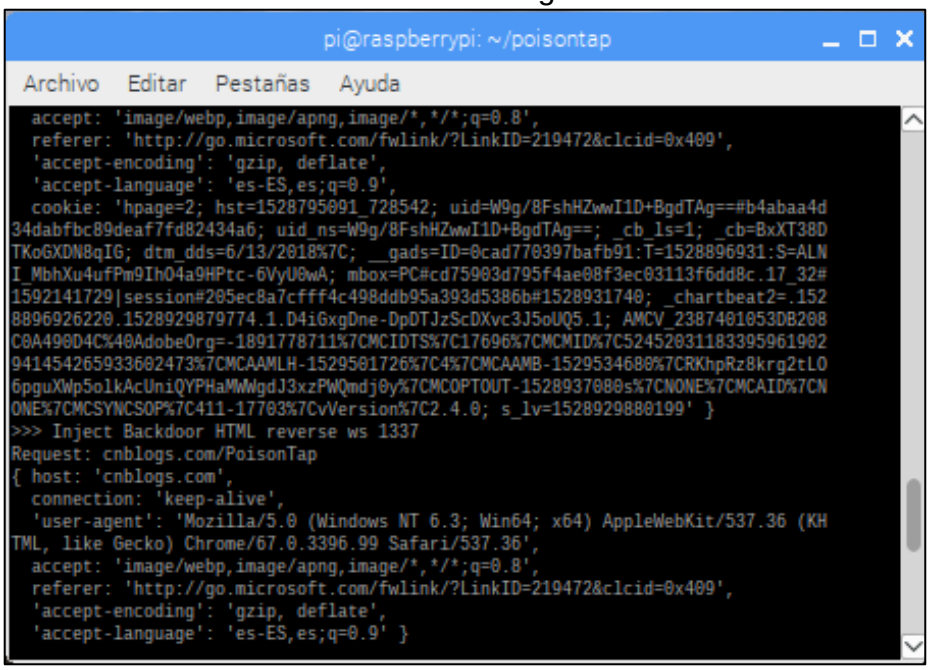
Gráfico No. 45 Verificación de la COOKIE de sesión



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

0En este caso se procede analizar la COOKIE de sesión verificando los números de sesiones que se han efectuado en el sistema informático, como se ve en el gráfico No. 46.

Gráfico No. 46 Verificación de la segunda COOKIE de sesión



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

ENTREGABLES DEL PROYECTO

Los entregables del proyecto son los siguientes:

- Diseño de la red de área local con el respectivo vector de ataque de POISONTAP.
- Configuración de la placa Raspberry PI Zero.
- Evidencias del vector de ataque POISONTAP.
- Evidencias de la empresa Marcelo Rúales donde se implementó el proyecto.

4.1.7 CRITERIOS DE VALIDACIÓN DE LA PROPUESTA

Este proyecto sobre el análisis de vulnerabilidades aplicando el mini ordenador Raspberry Pi Zero Poisontap es de gran validez debido a que por medio de esta placa se demostrará las vulnerabilidades presentes en la red de área local de la empresa Marcelo Rúales con el objetivo de determinar medidas de protección en las estaciones de trabajo que se conectan a la red, además este Hardware proporcionará diferentes ataques como el Backdoor que serán utilizados en el momento de ejecutar las pruebas de Hackeo ético en las computadoras conectadas a la red LAN, para finalmente gestionar un informe presentando todos los resultados basados en el Hackeo de la red de datos a través de Poisontap.

Durante la ejecución de este análisis de vulnerabilidades se dictaminará cuáles son las medidas de protección en lo cual serán recopiladas por medio de expertos de seguridad informática donde se proporcionarán como mitigar los riesgos y las amenazas presentes en las redes LAN a través de una tabla detallando la funcionalidad de cada medida de seguridad, con la finalidad de reducir los índices de ataques cibernéticos.

4.1.8 CRITERIOS DE ACEPTACIÓN DEL PRODUCTO

La aceptación de esta propuesta se debe al requerimiento de ejecutar un análisis de vulnerabilidades por medio de la minicomputadora Raspberry PI Zero determinado así el nivel de impacto que estas pueden producir al momento de ser explotadas por piratas informáticos.

Tabla No. 16 Criterios de Aceptación del Producto o Servicio

Indicadores				
Descripción	**Si Cumple**	**No Cumple**	**Indiferente**	**Desconozco**
Instalación del sistema operativo NOOBS Debían en el Raspberry PI Zero.	**X**			
Configuración de Poisontap en el Raspberry PI Zero.	**X**			
Diseño de red del vector de ataque Poisontap.	**X**			
Ejecución de las pruebas de ataque por medio de la placa Raspberry PI Zero	**X**			

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Tabla No. 17 Criterios de Aceptación del Producto II

Indicadores				
Descripción de los capítulos	**Revisado y aprobado por el Tutor**	**Observaciones por el tutor**	**Informe del tutor por falla de los estudiantes**	**Indiferente**
Elaboración de la introducción.	✓			
Identificación del problema, causas y consecuencias, delimitación del problema, objetivos de la investigación, alcances problema y justificación e importancia.	✓			
Elaboración del marco teórico, antecedentes de estudio, fundamentación teórica, legal y definiciones conceptuales.	✓			
Definición de la factibilidad operacional, técnica, económica, legal e implementación del proyecto aplicando una metodología.	✓			
Elaboración de los criterios de aceptación del producto o servicio, las conclusiones y recomendaciones	✓			

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

A través de un estudio realizado se pudo determinar que el miniordenador Raspberry PI Zero es de vital importancia ya que por medio de este se pueden explotar vulnerabilidades de puertos USB de estaciones de trabajo conectadas a una red, una de las funcionalidades que la placa Poisontap realiza es la ejecución de ataques pasivos que permiten la captura de tráfico generado en una computadora mediante el puerto USB.

El objetivo de este proyecto de titulación es dar a conocer la importancia de proteger los puertos USB en las computadoras y servidores físicos debido a que los piratas informáticos poseen la capacidad de efectuar una combinación de ataques para lograr conectar la placa electrónica Poisontap en un servidor sea: WEB, Directorio Activo y Bases de Datos con la finalidad de acceder a la información confidencial de forma física produciendo daños en la confidencialidad e integridad de los datos ya que una vez obtenido los registros los atacantes pueden modificarlos.

Para llevar a cabo la presentación de la propuesta tecnológica se realizaron una serie de pruebas con la Raspberry PI Poisontap partiendo desde la instalación del sistema operativo NOOBS hasta lograr la ejecución de los paquetes que conforman el Poisontap.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Por medio de un levantamiento de información se detalló que en la oficina donde se realizó la prueba de ataque está compuesta por seis ordenadores que se conectan a un Switch que les proporciona el servicio de internet y se verifico que en las estaciones de trabajo se encontró un nivel de seguridad bajo en el cual los usuarios dejaban sus sesiones abiertas y el sistema no poseía la función de cierre de sesión automático además, también se detectó que los puertos USB no estaban bloqueados exponiendo las computadoras a cualquier intrusión maliciosa a través de puerto USB, las máquinas no cuentan con un control de acceso y antivirus actualizado.

- La prueba de ataque que se realizó a través de la placa Raspberry PI Zero, se asemeja a una intrusión de hombre en el medio ya que la placa captura el tráfico generado en un ordenador y además esta intrusión se la denomina pasiva por lo cual solamente intercepta paquetes para la detección de credenciales de usuario que trae como consecuencia provocar accesos ilícitos a la información violentando así la confidencialidad de los datos.

- Durante la realización de la Auditoría de Seguridad Informática se presenta las posibles recomendaciones como: bloqueo de puertos USB, activación de navegación incógnita y la ejecución de túneles VPN garantizando la disminución de los riesgos que pueden ser provocados por medio de Poisontap.

RECOMENDACIONES

- Proponer una evaluación de seguridad de los ordenadores que se conectan a una red de datos, estableciendo controles que ayuden a disminuir los riesgos que pueden ser provocados por medio de la placa Raspberry PI Zero.

- Aplicar controles de seguridad como capacitaciones permanentes al personal, bloqueo de puertos Usb, mantener el equipo y antivirus actualizado con el fin de evitar la propagación de ataques de intercepción de paquetes que provocan la captura de credenciales de usuarios y de accesos no autorizados a los sistemas informáticos.

- Proponer medidas de protección basadas en las normas ISO 27001, A.12.6.1 Gestión de vulnerabilidades técnicas, A.11.1.1 Control de perímetro de seguridad Física, A.11.1.2 Control Físico de los ingresos, en seguridad de la información que permitan establecer controles en los riesgos y una mitigación de estos con el objetivo de no provocar incidentes de seguridad.

BIBLIOGRAFÍA

Antonio, F., Forero, M., Manuel, J., & Garcia, S. (2016). Una nueva experiencia en seguridad hacking ético, 1–35.

Coello, Á., & Alejandrina, L. (2017). DISEÑO DE UNA APLICACIÓN SEGURA DE MENSAJERÍA WEB INTERNA UTILIZANDO EL ALGORITMO DE ENCRIPTACIÓN RSA PARA LA CARRERA DE INGENIERÍA EN NETWORKING & TELECOMUNICACIONES, AÑO 2017.

David Galisteo, R. M. (2012). Ataques MITM.

Gonzalez, J. (2016). ANÁLISIS Y COMPORTAMIENTO DE UN BUS PIRATE PARA EL HACKING DE HARDWARE EN LOS DECODIFICADORES DE TV PRIVADA SATELITAL DTH PARA LA OPERADORA DIRECTV UBICADA EN LA CIUDAD DE GUAYAQUIL.

Granda, L. S.-K. (2016). “ANÁLISIS DE VULNERABILIDADES DEL PROTOCOLO SSL/TLS EN LAS PÁGINAS WEB GUBERNAMENTALES DEL ECUADOR MAS USADAS EN LA CARRERA DE INGENIERIA EN NETWORKING Y TELECOMUNICACIONES.”

Himanen, P. (2013). La ética del hacker y el espíritu de la era de la información. *Tecnology*, *XVII*(1), 166. Retrieved from http://hdl.handle.net/10760/12851

Mieres, J. (2013). Ataques informáticos, 17. Retrieved from www.evilfingers.com

Ochoa, M. (2013). Seguridad Física , prevención y detección, 110–113.

Palomeque, D. P.-Y. (2013). keylogger.

Ramos Ramos, L. J. (2014). Pruebas De Penetración O Pent Test. *Revistasbolivianas*, 31–33. Retrieved from http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a14.pdf

Tiempo, D. el. (2015). Delitos Informáticos. Retrieved from http://www.eltiempo.com/archivo/documento/CMS-16493604

Universo, D. el. (2013). Fraude Informatico. Retrieved from https://www.eluniverso.com/noticias/2013/11/26/nota/1821096/bancos-pagaron-clientes-2-mil-casos-fraude-virtual

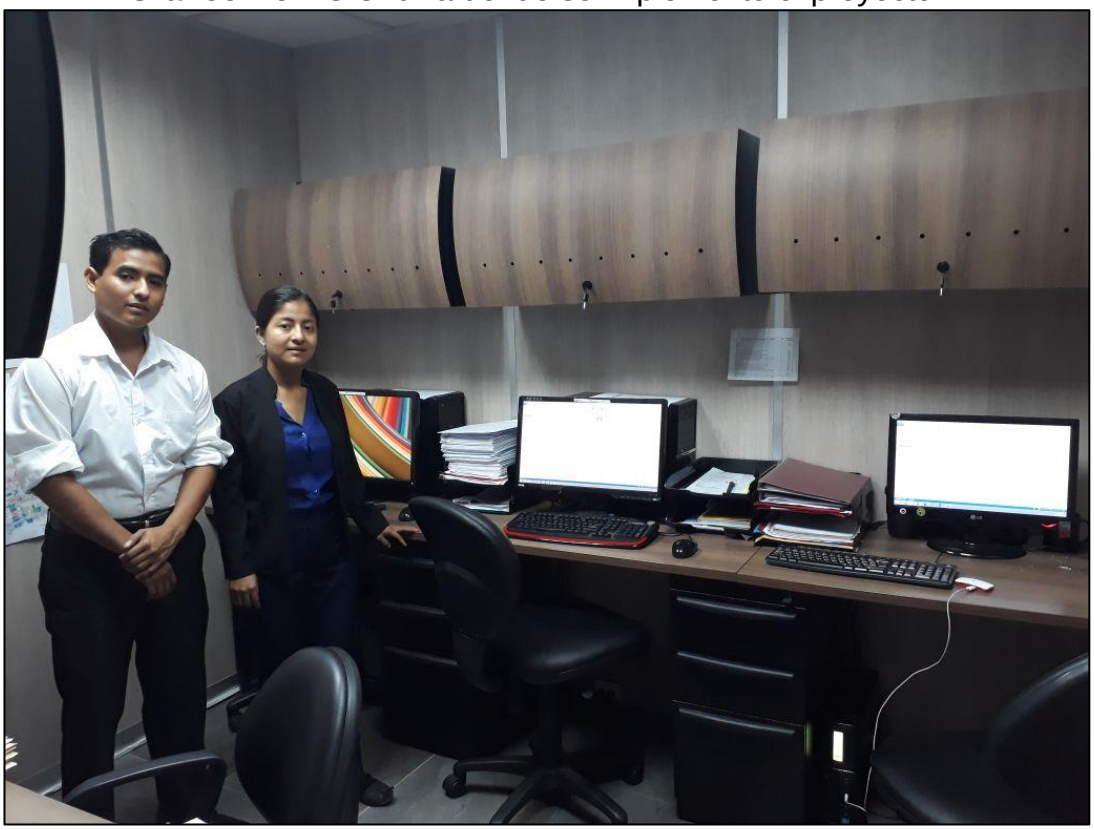
ANEXOS

Anexo I: Empresa donde se implementó el proyecto.

Gráfico No. 47 Entrada de la Oficina

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

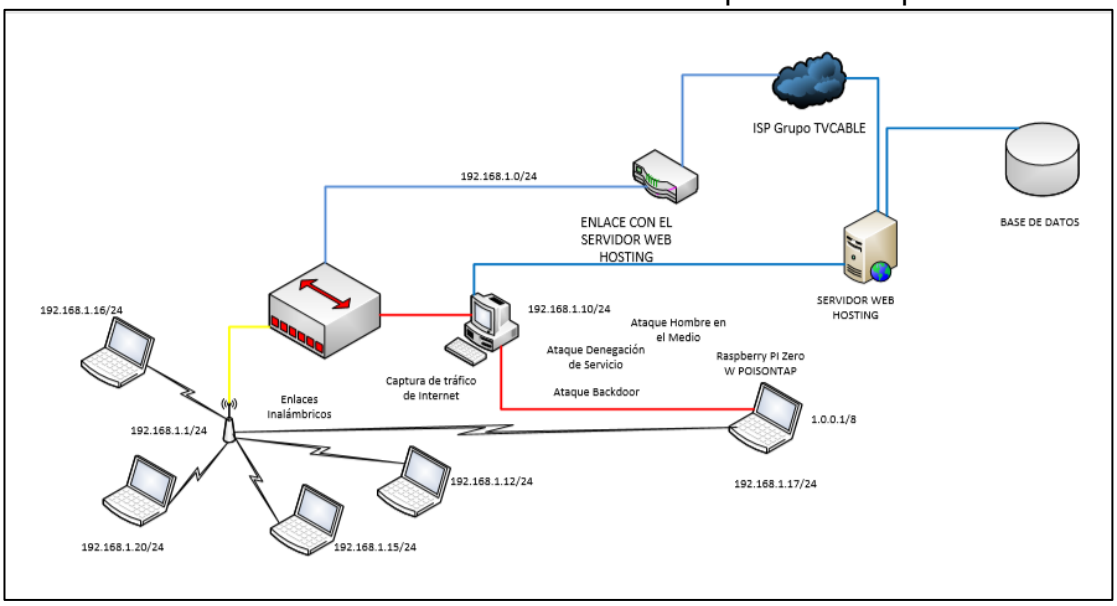
Gráfico No. 48 Oficina donde se implementó el proyecto



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

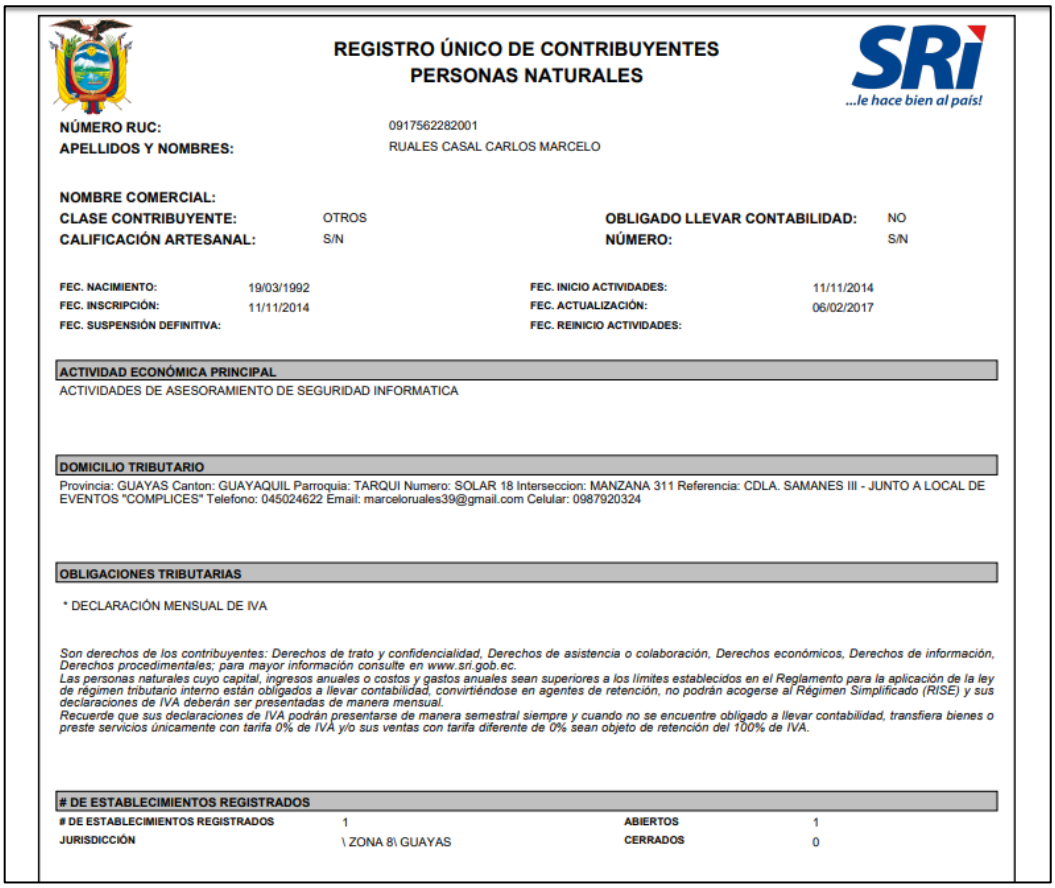
Anexo II: Diseño de red del ataque.

Gráfico No. 49 Diseño del vector de ataque Poisontap



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 50 RUC DE LA EMPRESA MARCELO RÚALES



REGISTRO ÚNICO DE CONTRIBUYENTES
PERSONAS NATURALES

...le hace bien al país!

NÚMERO RUC: 0917562282001
APELLIDOS Y NOMBRES: RUALES CASAL CARLOS MARCELO

NOMBRE COMERCIAL:
CLASE CONTRIBUYENTE: OTROS
CALIFICACIÓN ARTESANAL: S/N
OBLIGADO LLEVAR CONTABILIDAD: NO
NÚMERO: S/N

FEC. NACIMIENTO: 19/03/1992
FEC. INSCRIPCIÓN: 11/11/2014
FEC. SUSPENSIÓN DEFINITIVA:
FEC. INICIO ACTIVIDADES: 11/11/2014
FEC. ACTUALIZACIÓN: 06/02/2017
FEC. REINICIO ACTIVIDADES:

ACTIVIDAD ECONÓMICA PRINCIPAL
ACTIVIDADES DE ASESORAMIENTO DE SEGURIDAD INFORMATICA

DOMICILIO TRIBUTARIO
Provincia: GUAYAS Canton: GUAYAQUIL Parroquia: TARQUI Numero: SOLAR 18 Interseccion: MANZANA 311 Referencia: CDLA. SAMANES III - JUNTO A LOCAL DE EVENTOS "COMPLICES" Telefono: 045024622 Email: marceloruales39@gmail.com Celular: 0987920324

OBLIGACIONES TRIBUTARIAS
* DECLARACIÓN MENSUAL DE IVA

Son derechos de los contribuyentes: Derechos de trato y confidencialidad, Derechos de asistencia o colaboración, Derechos económicos, Derechos de información, Derechos procedimentales; para mayor información consulte en www.sri.gob.ec.
Las personas naturales cuyo capital, ingresos anuales o costos y gastos anuales sean superiores a los límites establecidos en el Reglamento para la aplicación de la ley de régimen tributario interno están obligados a llevar contabilidad, convirtiéndose en agentes de retención, no podrán acogerse al Régimen Simplificado (RISE) y sus declaraciones de IVA deberán ser presentadas de manera mensual.
Recuerde que sus declaraciones de IVA podrán presentarse de manera semestral siempre y cuando no se encuentre obligado a llevar contabilidad, transfiera bienes o preste servicios únicamente con tarifa 0% de IVA y/o sus ventas con tarifa diferente de 0% sean objeto de retención del 100% de IVA.

 # DE ESTABLECIMIENTOS REGISTRADOS
 # DE ESTABLECIMIENTOS REGISTRADOS 1
ABIERTOS 1
JURISDICCIÓN \ ZONA 8\ GUAYAS
CERRADOS 0

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 51 RUC de la EMPRESA MARCELO RÚALES

REGISTRO ÚNICO DE CONTRIBUYENTES
PERSONAS NATURALES

SRi ...le hace bien al país!

NÚMERO RUC: 0917562282001
APELLIDOS Y NOMBRES: RUALES CASAL CARLOS MARCELO

ESTABLECIMIENTOS REGISTRADOS

No. ESTABLECIMIENTO: 001 **Estado:** ABIERTO - MATRIZ **FEC. INICIO ACT.:** 11/11/2014
NOMBRE COMERCIAL: **FEC. CIERRE:** **FEC. REINICIO:**
ACTIVIDAD ECONÓMICA:
ACTIVIDADES DE ASESORAMIENTO DE SEGURIDAD INFORMATICA
ACTIVIDADES DE SOPORTES E INSTALACION DE REDES INFORMATICAS
SERVICIOS DE ASESORIA E INSTALACION DE SISTEMAS DE TELECOMUNICACIONES
ACTIVIDADES DE AUDITORIA EN SEGURIDAD INFORMATICA
DIRECCIÓN ESTABLECIMIENTO:
Provincia: GUAYAS Canton: GUAYAQUIL Parroquia: TARQUI Ciudadela: SAMANES III Numero: SOLAR 18 Referencia: JUNTO A LOCAL DE EVENTOS "COMPLICES" Manzana: 311 Celular: 0994267740 Telefono Domicilio: 045024622 Email: marceloruales39@gmail.com

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Anexo III: Recomendación principal basada en la norma ISO 27001.

Tabla No. 18 Recomendación principal de la ISO 27001

Vulnerabilidad	Control	Recomendación
Vulnerabilidad de explotación del puerto USB.	A.12.6.1 Control de vulnerabilidades técnicas	Se debe obtener de forma oportuna información sobre los fallos de seguridad de los puertos USB y tomar medidas adecuadas para obtener un control de los riesgos asociados. Generalmente la mayoría de las veces no es viable llegar a la eliminación total del riesgo, ya que podría ser imposible técnicamente o bien porque la empresa concluya que no es un riesgo suficientemente crítico. En estos casos la empresa puede aceptar el riesgo, ser consciente de que la amenaza para la información existe y dedicarse a monitorearlo con el fin de controlarlo. En definitiva, se trata de implantar las medidas preventivas o correctivas necesarias con el fin de reducir la posibilidad de ocurrencia o el impacto de riesgo.
Perímetro de Seguridad Física	A.11.1.1 Control de perímetro de seguridad Física	Se debe determinar y utilizar los perímetros de seguridad para proteger las áreas que contienen información sumamente confidencial y critica y las instalaciones donde se realiza el procesamiento de datos.
Control Físico de los Ingresos	A.11.1.2 Control Físico de los ingresos	Se debe proteger las áreas seguras mediante controles adecuados con el objetivo de garantizar el ingreso de personal autorizado a departamentos que contengan datos sumamente críticos.

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Anexo IV: Lista de ataques que se pueden realizar por medio de Poisontap

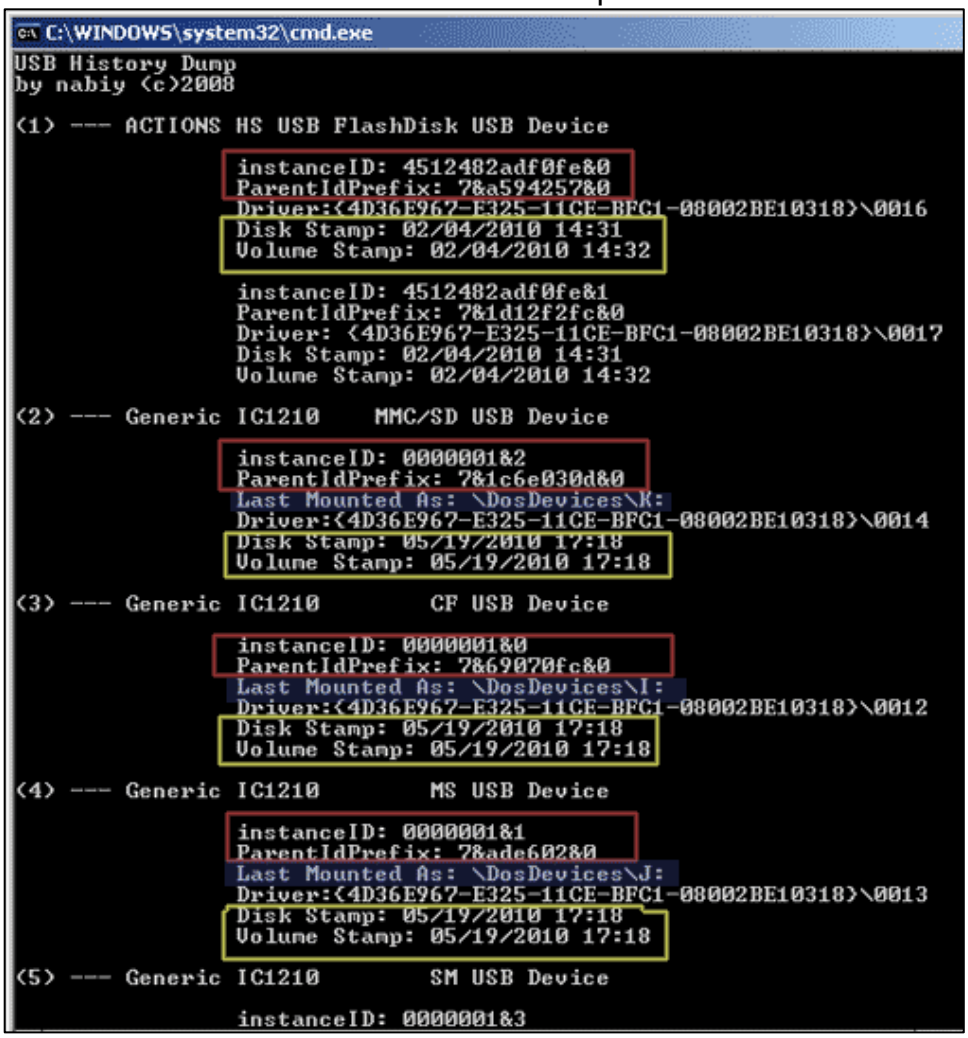
Tabla No. 19 Tipos de Ataques de Poisontap

Tipo de Ataque	Descripción
Denegación de Servicio	Consiste en limitar el acceso a la red a un dispositivo cliente, además estos ataques sobrecargan un servidor por el exceso de peticiones enviadas por los usuarios.
Hombre en el Medio	Este ataque cumple con la función de capturar tráfico en la red de datos logrando interceptar credenciales de usuario.
Ataque de autenticación al enrutador	Este ataque provoca una denegación total del servicio de internet colapsando el enrutador.
Ataque de Suplantación	Consiste en suplantar el servidor DHCP provocando él envió de solicitudes de respuesta falsas a los dispositivos clientes.
Ataque de Puerta Trasera	Consiste en inyectar un virus provocando un acceso indebido a la información almacenada en el navegador.

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Anexo V: Auditoría de Puertos USB

Gráfico No. 52 Auditoría de puertos USB

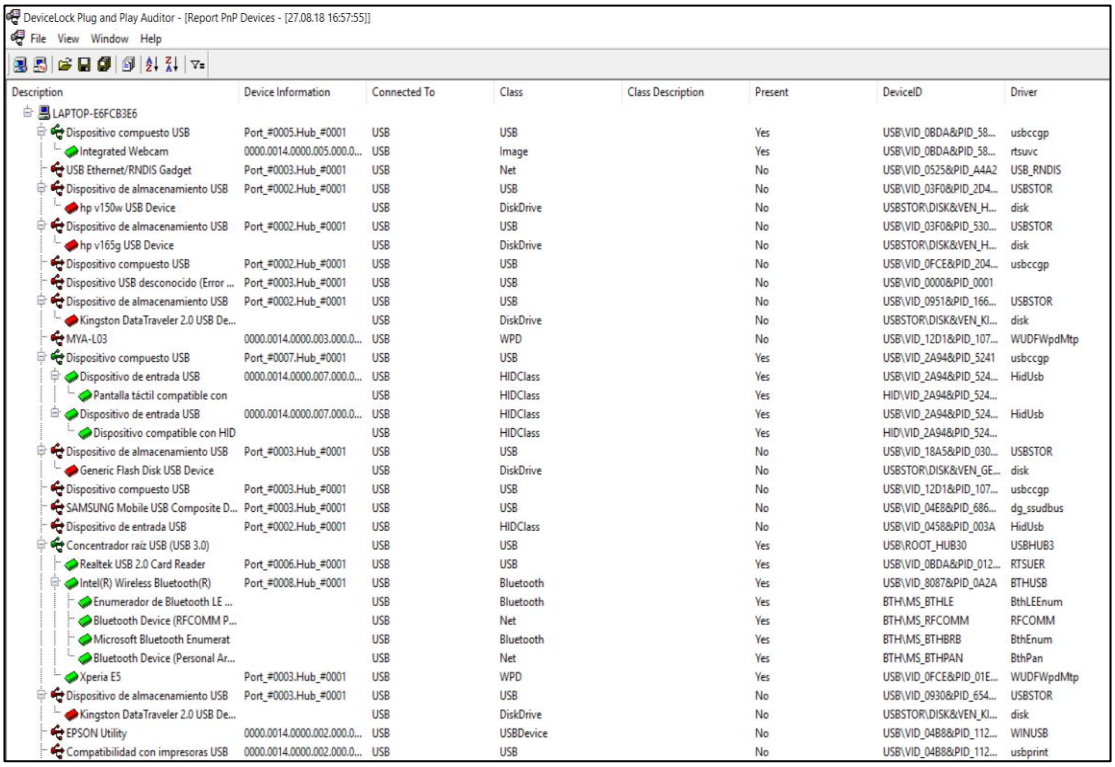


Fuente: https://seguridadyredes.wordpress.com/2010/05/19/auditando-puertos-usb-y-otros-dispositivos-registro-de-windows-y-software-dedicado/

Autor: Organización Alfon

En este caso se realiza un escaneo de los puertos USB a través de la herramienta USB AUDITOR.

Gráfico No. 53 Escaneo de conexiones USB

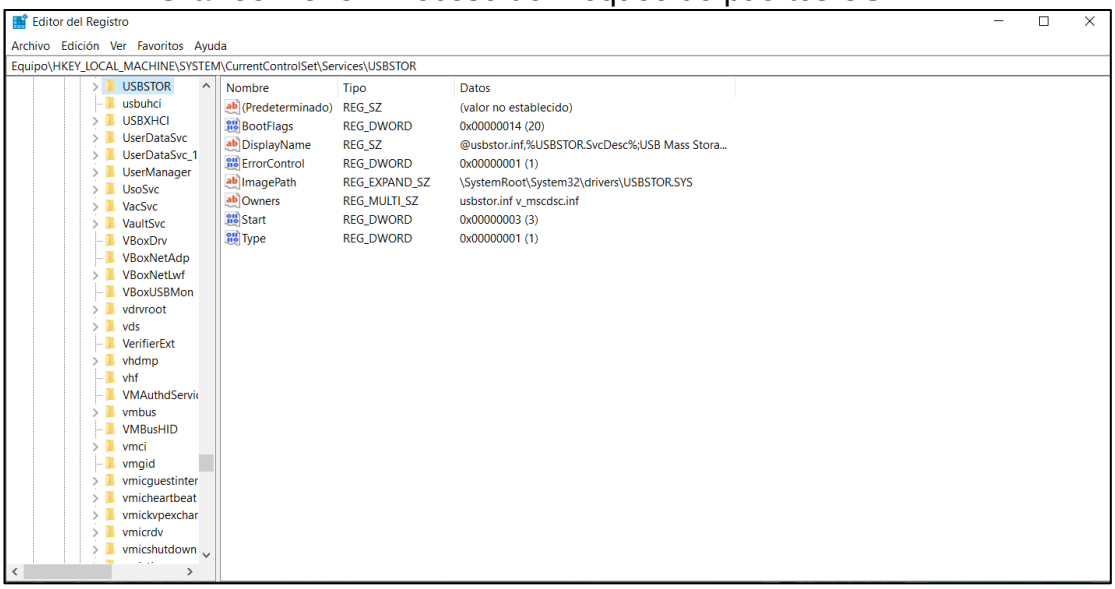


Description	Device Information	Connected To	Class	Class Description	Present	DeviceID	Driver
LAPTOP-E6FCB3E6							
Dispositivo compuesto USB	Port_#0005.Hub_#0001	USB	USB		Yes	USB\VID_0BDA&PID_58...	usbccgp
Integrated Webcam	0000.0014.0000.005.000.0...	USB	Image		Yes	USB\VID_0BDA&PID_58...	rtsuvc
USB Ethernet/RNDIS Gadget	Port_#0003.Hub_#0001	USB	Net		No	USB\VID_0525&PID_A4A2	USB_RNDIS
Dispositivo de almacenamiento USB	Port_#0002.Hub_#0001	USB	USB		No	USB\VID_03F0&PID_2D4...	USBSTOR
hp v150w USB Device		USB	DiskDrive		No	USBSTOR\DISK&VEN_H...	disk
Dispositivo de almacenamiento USB	Port_#0002.Hub_#0001	USB	USB		No	USB\VID_03F0&PID_530...	USBSTOR
hp v165g USB Device		USB	DiskDrive		No	USBSTOR\DISK&VEN_H...	disk
Dispositivo compuesto USB	Port_#0002.Hub_#0001	USB	USB		No	USB\VID_0FCE&PID_204...	usbccgp
Dispositivo USB desconocido (Error ...	Port_#0003.Hub_#0001	USB	USB		No	USB\VID_0000&PID_0001	
Dispositivo de almacenamiento USB	Port_#0002.Hub_#0001	USB	USB		No	USB\VID_0951&PID_166...	USBSTOR
Kingston DataTraveler 2.0 USB De...		USB	DiskDrive		No	USBSTOR\DISK&VEN_KI...	disk
MYA-L03	0000.0014.0000.003.000.0...	USB	WPD		No	USB\VID_12D1&PID_107...	WUDFWpdMtp
Dispositivo compuesto USB	Port_#0007.Hub_#0001	USB	USB		Yes	USB\VID_2A94&PID_5241	usbccgp
Dispositivo de entrada USB	0000.0014.0000.007.000.0...	USB	HIDClass		Yes	USB\VID_2A94&PID_524...	HidUsb
Pantalla táctil compatible con		USB	HIDClass		Yes	HID\VID_2A94&PID_524...	
Dispositivo de entrada USB	0000.0014.0000.007.000.0...	USB	HIDClass		Yes	USB\VID_2A94&PID_524...	HidUsb
Dispositivo compatible con HID		USB	HIDClass		Yes	HID\VID_2A94&PID_524...	
Dispositivo de almacenamiento USB	Port_#0003.Hub_#0001	USB	USB		No	USB\VID_18A5&PID_030...	USBSTOR
Generic Flash Disk USB Device		USB	DiskDrive		No	USBSTOR\DISK&VEN_GE...	disk
Dispositivo compuesto USB	Port_#0003.Hub_#0001	USB	USB		No	USB\VID_12D1&PID_107...	usbccgp
SAMSUNG Mobile USB Composite D...	Port_#0003.Hub_#0001	USB	USB		No	USB\VID_04E8&PID_686...	dg_ssudbus
Dispositivo de entrada USB	Port_#0002.Hub_#0001	USB	HIDClass		No	USB\VID_0458&PID_003A	HidUsb
Concentrador raíz USB (USB 3.0)		USB	USB		Yes	USB\ROOT_HUB30	USBHUB3
Realtek USB 2.0 Card Reader	Port_#0006.Hub_#0001	USB	USB		Yes	USB\VID_0BDA&PID_012...	RTSUER
Intel(R) Wireless Bluetooth(R)	Port_#0008.Hub_#0001	USB	Bluetooth		Yes	USB\VID_8087&PID_0A2A	BTHUSB
Enumerador de Bluetooth LE ...		USB	Bluetooth		Yes	BTH\MS_BTHLE	BthLEEnum
Bluetooth Device (RFCOMM P...		USB	Net		Yes	BTH\MS_RFCOMM	RFCOMM
Microsoft Bluetooth Enumerat		USB	Bluetooth		Yes	BTH\MS_BTHBRB	BthEnum
Bluetooth Device (Personal Ar...		USB	Net		Yes	BTH\MS_BTHPAN	BthPan
Xperia E5	Port_#0003.Hub_#0001	USB	WPD		Yes	USB\VID_0FCE&PID_01E...	WUDFWpdMtp
Dispositivo de almacenamiento USB	Port_#0003.Hub_#0001	USB	USB		No	USB\VID_0930&PID_654...	USBSTOR
Kingston DataTraveler 2.0 USB De...		USB	DiskDrive		No	USBSTOR\DISK&VEN_KI...	disk
EPSON Utility	0000.0014.0000.002.000.0...	USB	USBDevice		No	USB\VID_04B8&PID_112...	WINUSB
Compatibilidad con impresoras USB	0000.0014.0000.002.000.0...	USB	USB		No	USB\VID_04B8&PID_112...	usbprint

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

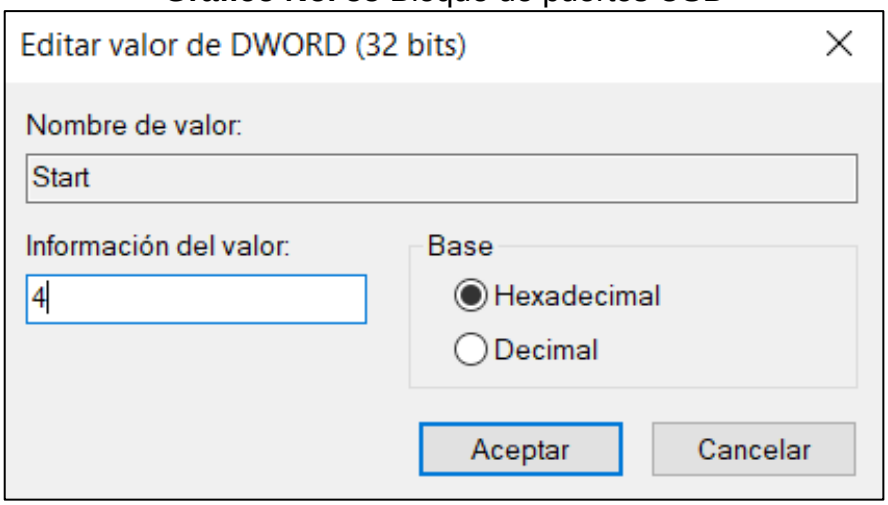
En este caso se procede a modificar el proceso del directorio USB TOR para bloquear los puertos modificando el número de puertos y el nombre de los archivos USBTOR y USBTOR.PNG, como se muestra en el gráfico No. 54, 55 y 56.

Gráfico No. 54 Proceso de Bloqueo de puertos USB



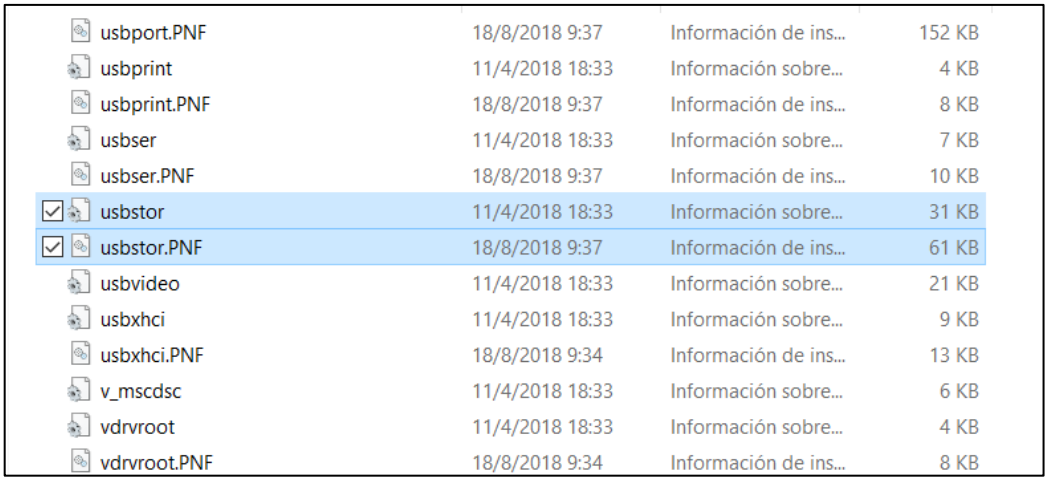
Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 55 Bloque de puertos USB



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 56 Cambios de nombre en el archivo



Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Dentro de este anexo se demuestra las alternativas de limitación del acceso a los puertos USB.

Gráfico No. 57 Removable Access Tool

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 58 Phrozen Safe USB

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

Gráfico No. 59 USB Flash Drives Control

Fuente: Trabajo de Investigación
Autores: Diana Cují-Mario Jalca

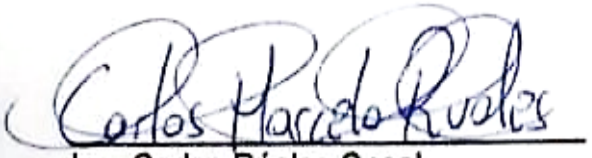
CARTA DE AUTORIZACIÓN

A quien corresponda:

Yo Ing. Carlos Marcelo Rúales Casal autorizo a los estudiantes de la carrera de Ingeniería en Networking y Telecomunicaciones, Mario Danilo Jalca Manzaba con cedula de ciudanía No. 0925676942 y Diana Shirley Cuji Toalombo con cedula de ciudadanía No. 0927354597, a que puedan implementar su proyecto de titulación basado en el Análisis de vulnerabilidades en la red de datos aplicando como mecanismo de test de intrusión la placa electrónica Raspberry PI Zero W Poisontap.

Este trabajo de titulación desarrollado cuyo tema **"ANÁLISIS DE LAS VULNERABILIDADES DE LA RED DE DATOS DE LA EMPRESA PYME "MARCELO RÚALES" DE LA CIUDAD DE GUAYAQUIL, UTILIZANDO LA HERRAMIENTA POISONTAP PARA EL HACKING ÉTICO E INYECCIÓN DE PUERTAS TRASERAS Y CAPTURA DE TRAFICO HTTP-HTTPS, INCORPORANDO LAS RECOMENDACIONES NECESARIAS PARA SU MITIGACIÓN."** es sumamente didáctico a través de un escenario de intrusión se demuestra el incidente de seguridad que se produce por medio de Poisontap.

Atentamente



Ing. Carlos Rúales Casal