Implementación de un sistema multifunción de tipo UTM utilizando hardware Atomic PI

Peñafiel Larco, Carlos Alejandro

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Trabajo de titulación, previo a la obtención del título de Ingeniero en Sistemas e Informática

Dr. Fuertes Díaz, Walter Marcelo

16 de septiembre del 2020

Resultados de Urkund

URKUND

Document Information

Analyzed document	Tesis_Carlos_Alejandro_Peñafiel_Larco_ID_L00326910.pdf (D79130339)
Submitted	9/14/2020 10:24:00 PM
Submitted by	Guerrero Idrovo Rosa Graciela
Submitter email	rgguerrero@espe.edu.ec
Similarity	3%
Analysis address	rgguerrero.espe@analysis.urkund.com

Sources included in the report

W	URL: https://repositorio.espe.edu.ec/bitstream/21000/9144/3/T-ESPEL-0889.pdf Fetched: 11/6/2019 5:40:36 PM	1
W	URL: https://latam.kaspersky.com/resource-center/definitions/utm Fetched: 9/14/2020 10:25:00 PM	3
SA	**Francis 15042020.docx** Document Francis 15042020.docx (D68262833)	1
W	URL: https://www.vmware.com/latam/topics/glossary/content/application-security.html Fetched: 9/14/2020 10:25:00 PM	4
SA	**tesis nuevo tema presentar.docx** Document tesis nuevo tema presentar.docx (D63525151)	1
W	URL: https://dspace.ucuenca.edu.ec/bitstream/123456789/22353/3/Tesis.pdf Fetched: 5/6/2020 8:06:14 PM	1

WALTER MARCELO FUERTES DIAZ

Firmado digitalmente por WALTER MARCELO FUERTES DIAZ
Nombre de reconocimiento (DN): c=EC, o=SECURITY DATA S.A. 1, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, serialNumber=0907201143 20, cn=WALTER MARCELO FUERTES DIAZ
Fecha: 2020.11.05 15:32:56 -05'00'

Dr. Fuertes Díaz, Walter Marcelo

C.C: 1707017701

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"Implementación de un sistema multifunción de tipo UTM utilizando hardware Atomic PI"*** fue realizado por el señor **Peñafiel Larco, Carlos Alejandro,** el cual ha sido revisado en su totalidad y analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustenten públicamente.

Sangolquí, 16 de septiembre de 2020

Firma:

WALTER MARCELO FUERTES DIAZ

Firmado digitalmente por WALTER MARCELO FUERTES DIAZ
Nombre de reconocimiento (DN): c=EC, o=SECURITY DATA S.A. 1, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, serialNumber=090720114320, cn=WALTER MARCELO FUERTES DIAZ
Fecha: 2020.11.05 15:33:39 -05'00'

Dr. Fuertes Díaz, Walter Marcelo

C.C: 1707017701

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

RESPONSABILIDAD DE AUTORÍA

Yo, **Peñafiel Larco, Carlos Alejandro,** con cédula de ciudadanía n° 1714988464, declaro que el contenido, ideas y criterios del trabajo de titulación: **Implementación de un sistema multifunción de tipo UTM utilizando hardware Atomic PI** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 16 de septiembre de 2020

Firma

1714988464 CARLOS ALEJANDRO PE¤ AFIEL LARCO

Firmado digitalmente por1714988464 CARLOS ALEJANDRO PE¤ AFIEL LARCO
DN: cn=1714988464 CARLOS ALEJANDRO PE¤ AFIEL LARCO gn=CARLOS ALEJANDRO c=EC l=QUITO o=PE¤ AFIEL LARCO CARLOS ALEJANDRO ou=Certificado de Representante Legal de Persona Juridica EC (FIRMA) e=carick_1986@hotmail.com
Motivo:Soy el autor de este documento
Ubicaci· n:
Fecha:2020-11-05 19:07-05:00

Peñafiel Larco, Carlos Alejandro

C.C. 1714988464

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

AUTORIZACIÓN DE PUBLICACIÓN

Yo, **Peñafiel Larco**, **Carlos Alejandro,** con cédula de ciudadanía n° 1714988464, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Implementación de un sistema multifunción de tipo UTM utilizando hardware Atomic PI** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 16 de septiembre de 2020

Firma

1714988464 CARLOS ALEJANDRO PE¤ AFIEL LARCO

Firmado digitalmente por1714988464 CARLOS ALEJANDRO PE¤ AFIEL LARCO
DN: cn=1714988464 CARLOS ALEJANDRO PE¤ AFIEL LARCO gn=CARLOS ALEJANDRO c=EC l=QUITO o=PE¤ AFIEL LARCO CARLOS ALEJANDRO ou=Certificado de Representante Legal de Persona Juridica EC (FIRMA) e=carick_1986@hotmail.com
Motivo:Soy el autor de este documento
Ubicaci· n:
Fecha:2020-11-05 19:07-05:00

Peñafiel Larco, Carlos Alejandro

C.C. 1714988464

Dedicatoria

Dedico a Dios el presente trabajo por proporcionarme de la fortaleza y sabiduría necesaria para poder culminar mi carrera profesional.

A mis Padres amados y hermanos por su apoyo incondicional.

Carlos Peñafiel

Agradecimiento

Agradezco a la Carrera de Sistemas de la Universidad de las Fuerzas Armadas "ESPE", porque en esta alma mater he recibido las buenas enseñanzas y el conocimiento, para llegar a la finalización de esta meta. Así mismo, a su distinguido personal académico el cual siempre forma excelentes profesionales del hoy y del mañana.

Un especial agradecimiento al Dr. Walter Fuertes, mi Director de tesis, quien me ha brindado su amistad y sobre todo su incondicional soporte con su vasto conocimiento en el área de la ciberseguridad.

A mis padres, les agradezco por su constante preocupación, amparo para que nunca me haga falta nada, su desvelo en las largas noches.

A mi hermano William, el que se encuentra en el cielo, donde no me desampara con sus abundantes bendiciones.

A mi hermano Richard, el cual es un pilar fundamental ya que con sus constantes bromas y preocupaciones sobre mi futuro han hecho de mí un hombre persistente y luchador.

¡A cuantas personas que fueron participes de mis logros, Muchas Gracias!

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

El presente estudio se llevó a cabo para cubrir la necesidad que tienen los hogares y pequeñas microempresas para la protección de datos. Para lograrlo, se diseñó y configuró en una placa electrónica de circuitos compacta o SBC (SINGLE BOARD COMPUTER) con una Gestión Unificada de Amenazas (Unified Threat Management, UTM) que ofrece algunas funcionalidades de protección de la información de bajo costo. Específicamente, tanto las funciones de detección y prevención de intrusos, como la de filtrado de contenido (firewalling). Para su ejecución se aplicó la Metodología de Investigación acción, y el uso de varias herramientas de hardware y software de código abierto (open-source) tanto para la recolección, inyección, filtrado y análisis de tráfico. Para las pruebas de concepto se utilizaron entornos virtuales de red controlados, sobre el cual se inyectaron diferentes tipos de ataques a la red. Los resultados demostraron la efectiva funcionalidad del UTM implementado sobre el hardware libre Atomic Pi.

- Palabras claves:
  - **UTM**
  - **ATOMIC PI**
  - **CLEAROS**
  - **METASPLOIT**

Abstract

This study was conducted to cover the need of households and small micro-enterprises for data protection. To carry out this, a Unified Threat Management (UTM) was designed and configured on a compact electronic circuit board (SBC), which offers some low-cost information protection functionalities. Specifically, both intrusion detection and prevention functions, as well as content filtering (firewalling). For its execution, the Action Research Methodology was applied, and the use of various hardware and open-source tools for the collection, injection, filtering, and analysis of traffic. A controlled virtual network environment was then used for the proofs of concept, on which different types of network attacks were injected. The results demonstrated the practical functionality of the UTM implemented on the free Atomic Pi hardware.

- Key words:
  - **UTM**
  - **ATOMIC PI**
  - **CLEAROS**
  - **METASPLOIT**

Capítulo I

Introducción

El actual capítulo se presenta una breve descripción de los antecedentes, objetivos, justificación y alcance del proyecto: “Esta investigación se enfocará en la implementación de dos funciones tales como son IDS e IPS de un producto UTM, sobre un Atomic Pi para una adecuada supervisión contra eventualidades que se presentan dentro de las organizaciones dotadas de infraestructura tecnológica”. Además, se expone una revisión sistemática de literatura sobre este tópico.

Antecedentes

La seguridad de la red es uno de los problemas más críticos causados por el anonimato en el ciberespacio. Entre los problemas que enfrenta el Internet de hoy, persiste el aumento de los delitos informáticos en su número y complejidad. Según (AMR, 2019), existen desarrollos importantes en el mundo de los ataques avanzados y los brotes epidémicos, por ejemplo, los ataques de WannaCry y ExPetr, difundidos en los titulares todo el mundo.

La primordial preocupación de las empresas es la seguridad de los datos. Cada vez los ingeniosos ataques, generalmente son operaciones de multicapa, lo que permite pasar desapercibidos a través de soluciones de protección endpoint, lo que deja a las empresas con una falsa sensación de seguridad cuando los delincuentes informáticos no dejan pistas o destruyen casi todos los rastros de su actividad (AMR, 2019).

Tradicionalmente las empresas, utilizan la solución de un firewall como primera línea de defensa. En un medio ambiente de red actual se torna cada vez más complicado la supervisión de

los ataques, razón por la cual el solo uso de un firewall no puede satisfacer las demandas tales como de rentabilidad, escalabilidad y convivencia con software de terceros. Por lo tanto, la implementación de UTM es esencial para las organizaciones.

De acuerdo con (Tam et al., 2012) un producto UTM puede solventar tres necesidades críticas: la necesidad de una mejor seguridad, necesidad de una seguridad más eficiente (desde el punto de vista de la ingeniería y también en costos) y la necesidad de tener una rentabilidad efectiva.

En concordancia con (Kaspersky, 2019), los productos UTM por lo general incluyen funciones tales como antivirus, antispyware, AntiSpam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas.

La compra de un dispositivo UTM para las organizaciones resulta excesivamente costoso, siendo inalcanzable su adquisición. La industria ha realizado soluciones como: Cisco, SonicWALL, Huawei, Sophos, Juniper Networks, Barracuda Networks, Stormshield, Venustech, Hillstone Networks, Untangle, Rohde & Schwarz Cybersecurity, WatchGuard.

Planteamiento del problema

El alto índice de los ataques cibernéticos a las organizaciones genera como consecuencia grandes pérdidas en las organizaciones. En Ecuador por ejemplo se registraron más de 40 millones de ataques cibernéticos, tras el retiro del asilo de Julián Assange (EL COMERCIO, 2019).

Por otro lado, en el Ecuador existe limitaciones profesionales especialistas en seguridad de la información, probablemente porque las universidades no tienen programas de posgrado en esta especialidad (Fuertes et al., 2014).

Además, las organizaciones no cuentan con suficiente tecnología de hardware y software para detectar y mitigar dichos ataques, probablemente por el alto costo de las herramientas, como es el caso de un UTM

Por lo expuesto, este proyecto tiene como propósito diseñar e implementar una solución de bajo costo que tenga la funcionalidad de un UTM utilizando IoT.

Justificación

Demostrar la adecuada implementación de las funcionalidades de UTM sobre un hardware IoT, caracterizada como una solución de bajo costo en la detección y mitigación de ataques cibernéticos que cumpla los estándares internacionales ISO 27000 y NIST (Iso27000.es, 2005).

Objetivos

Objetivo general

Desarrollar un prototipo de sistema de seguridad multifunción basado en la solución UTM, utilizando Hardware libre, para incrementar la seguridad de red de las organizaciones y los usuarios.

Objetivos específicos

- Determinar el estado del Arte, la funcionalidad de un UTM, y el diseño de la solución IoT.
- Construir un escenario controlado de pruebas para obtener información necesaria para cotejar con los indicios de la investigación.
- Dotar de funcionalidades UTM al dispositivo Atomic Pi, tales como Firewall, IDS e IPS usando el software ClearOs, Snort, Nessus y las librerías que ofrece el lenguaje Python para el Hardware Atomic Pi.

Alcance

Esta investigación se enfocará en la implementación de 2 funciones como son IDS e IPS de un producto UTM, sobre un Atomic Pi para una adecuada supervisión contra eventualidades que se presentan dentro de las organizaciones dotadas de infraestructura tecnológica.

Estado del arte

Se llevó a cabo un estudio sistemático a la literatura y trabajos relacionados con el tema de investigación para establecer el estado del arte, para lo cual se presentan varias preguntas de investigación afines a los objetivos específicos, tales como se muestra en la Tabla 1. Además, la estructura utilizada para la elaboración del estado del arte se muestra en la Figura 1.

Tabla 1

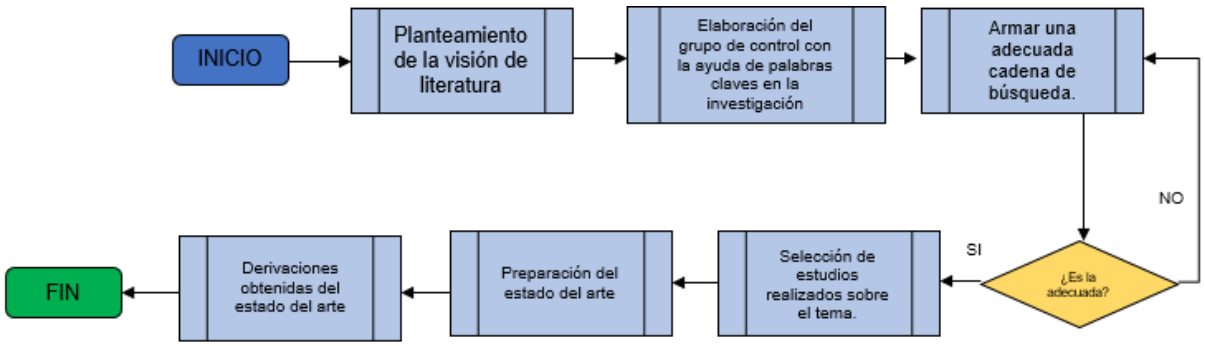
Preguntas de investigación

	Objetivo específico	Preguntas de Investigación
I.	**Determinar el estado del Arte, la funcionalidad de un UTM, y el diseño de la solución IoT**.	a. ¿Cómo se encuentra el estado del arte? b. ¿Cuál es el diseño de más adecuado para la solución IoT?
II.	**Construir un escenario controlado de pruebas para obtener información necesaria para cotejar con los indicios de la investigación.**	c. ¿Qué escenario virtual es el más adecuado para su implementación? d. ¿Cómo se puede verificar la eficacia de las funcionalidades implementadas? e. ¿Qué insumos debe tener el escenario para sus efectivas pruebas?

	Objetivo específico	Preguntas de Investigación
III.	**Dotar de funcionalidades UTM al dispositivo Arduino, tales como IDS e IPS usando el software Snort y las librerías que ofrece el lenguaje Python para el Hardware Arduino.**	f. ¿Cómo dotar de funcionalidades UTM a un dispositivo IoT mediante Snort? b. ¿Qué versión de Snort tiene más compatibilidad con las librerías de Python y Arduino?
IV.	**Analizar los resultados obtenidos a partir de la implementación del prototipo en la infraestructura de pruebas.**	g. ¿Resultó efectiva la implementación del dispositivo IoT?

Figura 1

Método para la elaboración del estado del arte



Planteamiento de la revisión de literatura

Esta fase se apoyó en la descripción del problema basado en los resultados descritos en el diagrama de "Causa y Efecto" de la figura 2, de tal manera de aportar con el contexto adecuado en la búsqueda de estudios científicos. Después de haber definido el objetivo de búsqueda y las correspondientes preguntas de investigación asociadas con esta temática, de tal manera poder definir los criterios adecuados de inclusión y exclusión.

Figura 2

Diagrama de Causa y Efecto

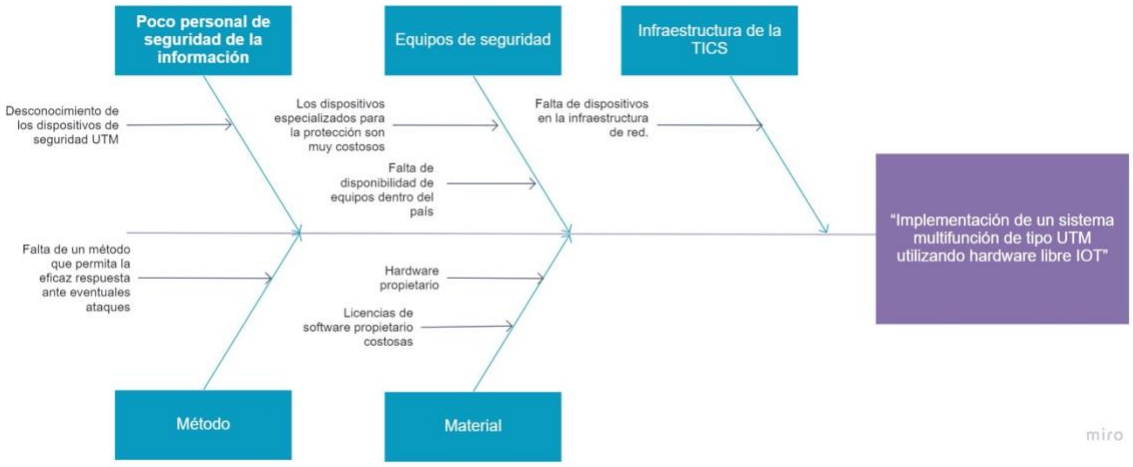


Tabla 2

Criterios de inclusión y de exclusión considerados

Inclusión	Exclusión
Uso de términos tales como: Eficiente sistema de respuesta contra ataques a los dispositivos IoT, UTM (Unified Threat Management), hardware libre como dispositivo de respuesta. Trabajos de investigación relacionados en inglés y en español. Solo trabajos realizados en el periodo comprendido entre 2015 -2016 Solo Scopus, IEEE, Springer.	Soluciones de respuesta contra ataques mediante hardware pagado.

Elaboración del grupo de control con la ayuda de palabras claves en la investigación

Con base a los problemas mencionados en el diagrama de causa y efecto, se pudo realizar una revisión de la literatura relevante no esquematizada, para lo cual se apoyó en 10 artículos relacionados al tema, de los cuales, se seleccionó 4 artículos relevantes que mencionan la importancia del uso de una solución de tipo UTM para las organizaciones, en la Tabla 3 se menciona el grupo de control.

Tabla 3

Grupo de control

Título	Cita	Palabras claves
Effective Utilization of Multicore Processor for Unified Threat Management Functions.	(Gummadi & Shanmugasundaram, 2012)	Performance analysis, URL filtering, spam filtering, Unified Threat Management (UTM), parallelization method
Improving Unified Threat Management Architecture Based on Net Channel Technology	(Hu, 2015)	UTM
¿Qué es la gestión unificada de amenazas (UTM)?	(Kaspersky, 2019)	UTM, VPN
UTM Security with Fortinet: Mastering Fort iOS.	(Tam et al., 2012)	Network security (firewalls to block unauthorized users, Intrusion Prevention Systems (IPS) to keep attackers out, Web filters to avoid misuse of Internet browsing, and antivirus software to block malicious programs)

Armar una adecuada cadena de búsqueda

Con las palabras claves utilizadas en los estudios antes revisados en el grupo de control se estructuro la siguiente cadena de búsqueda:

(("UTM" OR "ARDUINO") AND ("IPS" OR "IDS") AND ("IOT")) la cual se utilizó en el repositorio digital Crossref y en Scholar Google sin respuesta alguna.

Al tener una nula respuesta se cambió la cadena de búsqueda como se muestra a continuación:

(("UTM" AND "ARDUINO") AND ("IPS" AND "IDS") AND ("IOT") OR ("FIREWALL"))

Selección de estudios realizados sobre el tema

La cadena seleccionada la misma se la empleo en la amplia base de repositorios científicos como es Google Scholar, obteniendo un resultado de 4 artículos relacionados con el tema a desarrollar. Este número se considera no suficiente, pero si adecuado para el análisis.

De los 4 artículos se aplicaron filtros, los cuales se describen a continuación:

1. **Fecha de publicación:** se tomó en consideración la similitud de los estudios planteados con el presente trabajo, hasta con 3 años de antigüedad.
2. **Tipo de estudio:** Se seleccionó solo estudios del tipo: Article, Conference, White Papers, proceeding.

Tabla 4

Artículos de estado del arte

Código	Título	Cita
EP1	Implementación de un sistema de gestión de seguridad de la información aplicado al tele monitoreo médico.	(Ramírez & Jiménez, 2016)
EP2	Implementación de un Firewall Construido a partir de software y una placa de circuitos compacta o SBC (Single Board Computer) en la empresa Taio Systems de la ciudad de Popayán	(Pareja, 2017)

Elaboración del estado del arte

EP1. Implementación de un sistema de gestión de seguridad de la información aplicado al tele monitoreo médico.

Este trabajo tuvo como objetivo el implementar un sistema de gestión de seguridad de la información aplicado al tele monitoreo médico. Para ello fue necesario la recopilación de información referente a redes inalámbricas de área corporal, el uso de la tele medicina en la sociedad y la relación con las Tics. Así mismo se analizó sobre la seguridad de red e información basada en la norma ISO 27001 para luego diseñar una estructura robusta que permita asegurar los datos transmitidos inalámbricamente, al mismo tiempo que se evaluaba e implementaba el sistema de Tele monitoreo médico. Fue preciso acudir al uso de placas electrónicas tales como Arduino UNO, plataforma de sensores ehealth y módulo wifi 232-B para realizar el tele monitoreo. Una vez establecida la transmisión se realizó una categorización de activos y análisis y gestión de riesgos sobre el sistema representando así un porcentaje de cumplimiento de 71% de los requerimientos; además de realizar una comparación del sistema prototipo MFSecuEhealth contra un sistema no gestionado con seguridad obteniendo una mejora en el rendimiento notable de 86.2%. Se concluye que al analizar los requerimientos del sistema se logró optimizar los recursos y sobre todo se aseguró el activo más importante de la organización, la información. Se recomienda que para analizar, gestionar y monitorear un sistema informático se comparen los mejores gestores de seguridad para garantizar que su implementación salvaguarden las bases de la seguridad; confidencialidad, integridad y disponibilidad.

EP2. Implementación de un Firewall Construido a partir de software y una placa de circuitos compacta o SBC (Single Board Computer) en la empresa Taio Systems de la ciudad de Popayán (Pareja, 2017)

El proyecto fue diseñar una solución que apoye la protección de datos en una red mediante la implementación de un Appliance de Seguridad Perimetral, con el uso de una placa Raspberry PI modelo 1 B y un firewall libre, IpFire. El trabajo realizado presentó un caso de éxito en la implementación del dispositivo en la empresa TaIO Systems de la ciudad de Popayán el cual fue concebido en un corto periodo de tiempo permitiendo apoyar en gran medida la protección de datos de la red de la empresa de una forma eficiente. Como propuesta adicional al proyecto se planteó evaluar el funcionamiento del firewall, para ello se conformó un ambiente de pruebas en el cual se usaron máquinas virtuales con servicios que pueden ser vulnerados mediante porciones de código malicioso o exploits, que afectan el correcto funcionamiento de los equipos, gracias al uso de las herramientas especializadas para el reconocimiento de vulnerabilidades en dispositivos se evaluó los servicios implementados para ejecutar algunas pruebas y comprobar el funcionamiento del dispositivo, con el fin de mejorar la configuración implementada para la empresa donde se ejecutó el proyecto. Por otra parte, se realizó un estudio del funcionamiento del firewall en el hardware usado, presentando buenos resultados logrando procesar todas las peticiones en tiempo real sin afectar el correcto funcionamiento de la red de la empresa TaIO Systems mediante las herramientas de monitoreo del firewall.

Resultados del estado del arte

Luego de haber realizado un exhaustivo análisis del estado del arte se llegó a las siguientes conclusiones: 1) Son escasos los trabajos realizados para la implementación de un dispositivo IoT

para el monitoreo de la infraestructura de red. 2) Un solo trabajo se enfoca en la utilización de las multifunciones de un producto UTM sobre la infraestructura de red.

Con el apoyo de los resultados obtenidos se puede concluir que la implementación de las funcionalidades de un producto UTM sobre un dispositivo IoT, resultará.

Capítulo II

Metodología de investigación

Este capítulo muestra la metodología se aplicó, considerando los métodos adecuados y técnicas. Posteriormente, se presenta una breve descripción del marco teórico, para lo cual se apega a la red de categorías la cual sustenta la investigación.

Metodología

En esta investigación, se encuadra dentro del marco de la metodología de la cuantitativa, razón por la cual se desea conocer y sustentar la eficacia de la implementación, mediante factores de datos recolectados, para en su posterior interpretarlos con la ayuda de la probabilidad y estadística. Y cumplir con el objetivo de la investigación el cual es *desarrollar un prototipo de sistema de seguridad multifunción basado en la solución UTM, utilizando Hardware libre IoT, para incrementar la seguridad de red de las organizaciones y los usuarios,* en seguida se examina la aplicabilidad de los métodos y técnicas.

Métodos de investigación

Metodología de investigación - acción

El termino Investigación – acción fue definido por primera vez por Kurt Lewin, medico, biólogo, psicólogo y filósofo alemán. El cual es conocido como el fundador de la psicología moderna, quien se interesó en la investigación de la psicología de los grupos y de las relaciones interpersonales.

En si la Investigación – acción es una forma de investigación la cual permite vincular el estudio de los problemas de un contexto adecuado haciendo uso de programas de respuesta social, de tal manera alcancen de forma conjunta los conocimientos y transformaciones sociales.

Según (Colmenares & E., 2017), define a la investigación-acción como "una forma da indagación introspectiva colectiva emprendida por participantes en situaciones sociales con objeto de mejorar la racionalidad y la justicia de sus prácticas sociales o educativas, así como su comprensión de esas prácticas y de las situaciones en que estas tienen lugar".

Metodología de investigación bibliográfica

Consiste en la revisión de material bibliográfica con respecto al tema del proyecto.

De acuerdo con (Flores et al., 2012) "depende fundamentalmente de la información que se recoge o consulta en documentos a los que se puede acudir como fuente o referencia en cualquier momento o lugar".

Metodología de investigación descriptiva

Se aplicará recolección de datos, predicción e identificación exacta de los eventos e incidentes, haciendo uso de métodos estadísticos para la adecuada interpretación de los datos recolectados.

Técnicas e instrumentos para la recolección de datos

Técnica documental

Esta técnica hace referencia a la parte conceptual de la experimentación en IS, es más orientada a la experimentación y replicación de técnicas de pruebas de software.

Técnicas e instrumentos para el procesamiento y análisis

Dentro de las exigencias de la sustentación de los datos obtenidos mediante la experimentación se utilizará los siguientes instrumentos para su procesamiento:

Nivel exploratorio

Al diagnosticar la incidencia de los ataques cibernéticos sobre el escenario virtual de pruebas.

Nivel descriptivo

Permite evaluar los datos obtenidos mediante las pruebas, encontrar la relación que existen entre ellos, identificar a que se deben los hallazgos y dar un criterio, concluir en base a los resultados obtenidos.

Nivel de asociación de variables

Esta investigación se la debe comprobar mediante la hipótesis, en la cual coexiste la variable independiente y la variable dependiente.

Antecedentes investigativos

La seguridad de la red es uno de los problemas más críticos causados por el anonimato en el ciberespacio. Entre los problemas que enfrenta el Internet de hoy, persiste el aumento de los delitos informáticos en su número y complejidad. Según (AMR, 2019), existen desarrollos importantes en el mundo de los ataques avanzados y los brotes epidémicos, por ejemplo, los ataques de WannaCry y ExPetr, difundidos en los titulares todo el mundo.

La primordial preocupación de las empresas es la seguridad de los datos. Cada vez los ingeniosos ataques, generalmente son operaciones de multicapa, lo que permite pasar

desapercibidos a través de soluciones de protección endpoint, lo que deja a las empresas con una falsa sensación de seguridad cuando los delincuentes informáticos no dejan pistas o destruyen casi todos los rastros de su actividad (AMR, 2019).

Tradicionalmente las empresas, utilizan la solución de un firewall como primera línea de defensa. En un medio ambiente de red actual se torna cada vez más complicado la supervisión de los ataques, razón por la cual el solo uso de un firewall no puede satisfacer las demandas tales como de rentabilidad, escalabilidad y convivencia con software de terceros. Por lo tanto, la implementación de UTM es esencial para las organizaciones.

De acuerdo con (Tam et al., 2012), un producto UTM puede solventar tres necesidades críticas: la necesidad de una mejor seguridad, necesidad de una seguridad más eficiente (desde el punto de vista de la ingeniería y también en costos) y la necesidad de tener una rentabilidad efectiva.

En concordancia con (Kaspersky, 2019), los productos UTM por lo general incluyen funciones tales como antivirus, antispyware, Anti-Spam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas.

La compra de un dispositivo UTM para las organizaciones resulta excesivamente costoso, siendo inalcanzable su adquisición. La industria a realizado soluciones como Cisco, SonicWALL, Huawei, Sophos, Juniper Networks, Barracuda Networks, Stormshield, Venustech, Hillstone Networks, Untangle, Rohde & Schwarz Cybersecurity, WatchGuard.

Capítulo III

Marco teórico

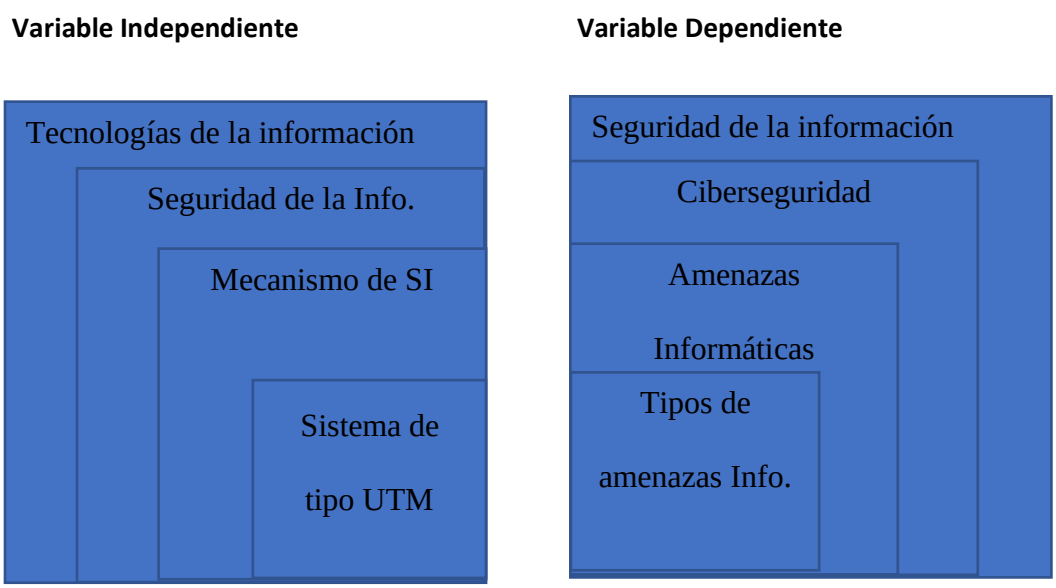
En este capítulo se menciona de algunos principios y conceptos básicos acerca de la seguridad de la información, Atomic PI, ClearO, Snort IDS, Snortsam, UTM,

Red de categorías

Es conveniente estructurar la red de las principales categorías que intervienen en este objeto de estudio; la red de categorías se muestra de la siguiente manera (ver Figura 3).

Figura 3

Red de Categorías de las variables de Investigación



Fundamentación científica de la variable independiente

Tecnologías de la información

Las Tics, son las tecnologías que se utilizan en la gestión y transformación de la información, y de manera particular es el uso de computadores y programas los cuales crean, modifican, almacenan, protegen y recuperan esa información.

Las TICs, hoy por hoy es un elemento esencial de la Sociedad de la Sociedad de la información con lo cual habilita la capacidad universal de acceder y contribuir a la información, las ideas y conocimiento. Por lo cual facilitan el intercambio y fortalecimiento del conocimiento mundial para la favorable evolución permitiendo un acceso controlado a la información para desarrollar las actividades culturales, educativas, económicas, sociales, políticas, sanitarias, oportunidades comerciales y el avance de las ciencias. Razón por lo cual es necesario conocer el concepto de la Seguridad de la información debido a la importancia que adquiere para la protección de la información (Duarte, 2008).

Seguridad de la información

La seguridad de la información permite asegurar la identificación, valoración y gestión de los activos de información y sus riesgos, en función del impacto que representan para una organización. Es un concepto amplio que no se centra en la protección de las TIC sino de todos los activos de información que son de un alto valor para la institución (Gummadi & Shanmugasundaram, 2012).

En este sentido, se debe entender a la seguridad de la información como un proceso integrado por un conjunto de estrategias, medidas preventivas y medidas reactivas que se ponen en práctica en las instituciones para proteger la información y mantener su confidencialidad,

disponibilidad e integridad de esta, dando como resultado la existencia de los diversos tipos de Soluciones de Seguridad de la Información(Gummadi & Shanmugasundaram, 2012).

Soluciones de seguridad de la información

Con la creciente demanda de estos últimos días por la necesidad de mantenerse conectados desde los hogares, ya sea para estudios virtuales, realizar transacciones bancarias, trabajos en modalidad a distancia, etc. Presenta un juego de dinámicas Estatales. Con ello aumenta la necesidad e importancia de propender por la seguridad informática o mejor conocida como ciberseguridad, también la encargada de la protección de la integridad y la privacidad de la información la cual se puede encontrar almacenada en un sistema informático, además esta se puede hallar transitando en la red de computadores.

Software empresarial

Es recomendable para una Pyme la adquisición de Software enfocado al sector empresarial y conocer el uso correcto, esto genera grandes beneficios tales como: mejora de la productividad, reducción de costos e incremento de las ventas. Para adquisición adecuada de estas soluciones hay que estar al tanto de las soluciones acorde al flujo del negocio. Esto presenta un desafío el saber invertir en soluciones apropiadas las cuales contribuyan en la administración de la información. Este Software debe ser robusto en la seguridad informática, teniendo en cuenta de que las Pymes hacen uso de los dispositivos móviles o también conocidos BYOD.

Sistema UTM

Es la gestión unificada de amenazas, es un término se utiliza dentro de la seguridad de la información la cual indica de que se trata de una solución de seguridad, comúnmente se trata de un único producto de seguridad el mismo que brinda varias funciones de protección en un solo punto de red. Por lo general esta solución cuenta con funciones tales como: antivirus,

antispyware, Anti-Spam, firewall de red, IDS, IPS, escáner de vulnerabilidades y filtrado de contenido.

Fundamentación científica de la variable dependiente

Seguridad de las aplicaciones

Hace referencia al proceso de desarrollar, añadir y probar características de seguridad dentro de las aplicaciones, con la finalidad de impedir vulnerabilidades de seguridad frente las amenazas, tales como la alteración y accesos no autorizados.

Es necesario la seguridad de las aplicaciones debido a que las aplicaciones actuales se encuentran disponibles atreves de varias redes y conectada a la Cloud. Lo que acarrean el aumento de vulnerabilidades y las amenazas de seguridad. Por esta razón se ha elevado la necesidad de garantizar la seguridad no solo a nivel de la red, debe contar con la seguridad dentro de las aplicaciones. Con ello se debe efectuar pruebas de seguridad a las aplicaciones y así descubrir puntos endebles de las aplicaciones, de esta manera evitar este tipo de ataques. Existen varios tipos de seguridad de las aplicaciones como son:

Seguridad de las aplicaciones en la cloud

Las aplicaciones que se encuentran alojadas en Cloud presentan un sinfín de desafíos. Debido a que los entornos Cloud entregan recursos compartidos, por esta razón se recomienda dar a los usuarios solo tengan acceso a datos autorizados. Siempre se debe considerar que los datos confidenciales son más vulnerables en las aplicaciones alojadas en la Cloud (VMware, 2020).

Seguridad de las aplicaciones móviles

Hay que tener en cuenta que los dispositivos móviles transmiten y adquieren información por medio del internet, todo esto se realiza sobre una red no privada; siendo vulnerables a ataques. Por estas razones es recomendable que las empresas agreguen VPN con ello podrán

añadir una capa de seguridad cada vez que los empleados desean comunicarse con sus aplicaciones de manera remota (VMware, 2020).

Seguridad de las aplicaciones web

Las aplicaciones web o servicios se acceden a través de una interfaz de un navegador por medio del internet. Aplicaciones orientadas a la Web siente se encuentra instaladas en servidor remoto, y a información es trasmitida al internet. Las empresas que albergan a las aplicaciones web optan por proteger su red contra intrusos mediante contrafuegos orientados a las aplicaciones Web. Los contrafuegos se encargan de inspeccionar los paquetes de entrada como también los paquetes de salida, si considera datos perjudiciales y si es necesario los bloquea (VMware, 2020).

Ciberseguridad

Constituye en la condición para permitir a los ciudadanos, las organizaciones e instituciones logren favorecer del uso del ciberespacio mediante el mismo puedan efectuarse de forma rápida y económica los intercambios de información. La ciberseguridad nace ante el constante crecimiento del uso del ciberespacio en la interacción social, resultado de la revolución tecnológica de la información y comunicación (Tics), lo que ha impulsado el proceso de la globalización y periódicamente es sorprendente su vertiginosa innovación.

Amenazas informáticas

Es cualquier hecho natural o maniobra de tipo técnico o humano, que implique alterar, obstaculizar, oponerse o destruir la información de la organización. Según (Cisco Systems, 2005), la define como un acceso no autorizado a la red o dispositivo. Existen diversos tipos de

clasificaciones respecto a las amenazas informáticas, las mismas que guardan alguna relación unas con otras.

Tipos de amenazas informáticas

Amenazas externas

Estas son ocasionadas fuera de la organización las cuales se encuentran clasificados los virus, gusanos, caballos de Troya, intentos de ataques piratas informáticos, relacionados con exempleados o también causados por espionaje industrial (Cisco Systems, 2005).

Amenazas internas

Este tipo de amenazas provienen desde el interior de la organización estas causan grandes pérdidas ya que pueden ser causadas por medio de elementos que se encuentran dentro de la organización, como por ejemplo esto se da cuando hay un empleado descontento y tiene un gran conocimiento de seguridad informática, además cuenta con las credenciales de esta para cumplir con sus fechorías (Cisco Systems, 2005).

Capítulo IV

Descripción del sistema

Este capítulo da a conocer de manera específica el software y hardware utilizados para el desarrollo del presente proyecto de titulación. También se describe el sistema operativo CelarOS empleado para la implementación de las funcionalidades de UTM dentro de la tarjeta Atomic PI.

Atomic Pi

Es una tarjeta SBC (SINGLE BOARD COMPUTER), que cuenta con características similares a la Raspberry Pi, la única gran diferencia lo tiene en su procesador central Intel Atom x5-Z8350 con arquitectura X86, siendo ideal para el soporte de sistemas operativos tanto en Linux como también Windows basados en esta arquitectura.

Además, cuenta con almacenamiento incorporado de 16GB, una ranura de expansión microSD con un soporte hasta 256GB de almacenamiento, 2GB de memoria RAM DDR3L, conector Ethernet, Wifi b/g/n/ac, un puerto USB y conectores GPIO (Manuti, 2019).

Figura 4

Tarjeta Atomic PI

Nota. (Manuti, 2019)

Snort IDS

Es un IDS más popular en estos días, cuenta con una gran base de datos de firmas de actividades maliciosas. Esto ayuda en la búsqueda de contenido específico en los flujos de la red y reporta cada instante de una firma en particular. Los datos llegan desde la red ingresando a al Packet Decoder de IDS. Los paquetes son preparados y enviados al Pre - procesador y para adaptarse a las necesidades del motor de detección, que analiza el paquete para detectar la existencia de alguna actividad de intrusión (Kyaw et al., 2016).

Los paquetes regulares se descartan mientras que los sospechosos registrados por el sistema de registro y alerta. Entonces, la salida del módulo acepta los registros y genera el resultado final.

Firewall

Por lo general, un Firewall puede ser Software o Hardware, o tal vez la combinación de los dos, que realizan el filtrado de la transmisión de paquetes de la información digital como paso atreves de una interfaz entre la red (Kyaw et al., 2016).

Existen dos tipos de funciones básicas de seguridad:

- Filtrado de paquetes: Orientado a permitir o negar el paso de los paquetes con información digital, basado en los estamentos de las políticas de las reglas de seguridad.
- Proxy de la aplicación: Provee de servicios para la red de usuarios mientras que protege a los al anfitrión principal del computador. Esto es para parar el flujo de la IP (tráfico de red entrante y saliente).

IDS

El detector de intrusos está compuesto de técnicas y métodos las cuales son empleadas en la detección de actividades a nivel de red y de host, Los sistemas de detección de fallas están comprendidos en dos categorías básicas como son: detección de intrusos basados en las firmas y detección de sistemas anómalos. Están con una gran cantidad firmas y reglas configuradas, el objetivo de los sistemas de detección es buscar y registrar la actividad sospechosa y generar alertas. En base de las anomalías usualmente depende del paquete de anomalías presente en el protocolo de la parte del encabezado. En algunos casos estos métodos producen buenos resultados comparados por basado con firmas IDS. Usualmente un sistema de detección captura de datos en la red y aplica estas reglas que los datos o detecta anormalidades en esto (Rehman, 2003).

IPS

El sistema de prensión de intrusos es un dispositivo aplicado en la seguridad informática, esencial en las redes, esta se encarga de supervisar las actividades en la capa de Red, además monitorea la capa de Aplicación, de esta manera encontrar conductas maliciosas, con la finalidad de actuar ante estos sucesos en tiempo real como medida de contingencia.

El IPS es complementario a otras herramientas de la seguridad informática para aumentar la protección de las redes, la reacción es proactivo frente amenazas y ataques.

Wireshark

Es un analizador de protocolos es empleado para solucionar y analizar problemas de las telecomunicaciones, para este trabajo se lo utilizó en la visualización de las pruebas realizadas sobre el dispositivo IoT (Wireshark, 2020).

Figura 5

Logo de Wireshark

Nota. (Wireshark, 2020)

Hping3

Es herramienta de análisis orientada para ser utilizado mediante línea de comandos utilizado en testeo de redes y hosts, está basada en el comando ping de UNIX, es compatible con los protocolos TCP, ICMP, RAW-IP y UDP.

Esta herramienta fue empleada en la elaboración de los ataques orientados a la maquina denominada Victima, de esta manera testear la eficacia de respuesta a incidentes (Sanfilippo, 2020).

Figura 6

Logo de Hping

Nota. (Sanfilippo, 2020)

ClearOS

En estos días existen muchos firewalls Linux de código abierto, tales como Mono Wall, Endian, IPCop, SmoothWll Express, etc.

Todos estos se ejecutan sobre un marco de netfilter dotado por Linux Kernel algunas distribuciones de Linux incluso implementan funcionalidades tales como Proxy, IDS y VPN para poder proporcionar una solución de seguridad más perfecta.

ClearOS es desarrollado por una acreditada organización llamada ClearFoundation la misma que cuenta con una comunidad de usuarios y es una distribución famosa según http://distrowatch.com la clasifican en la posición 52.

ClearOS también conocida como ClakConnect es una distribución de Linux basada en CentOS y Red Hat Enterprise.

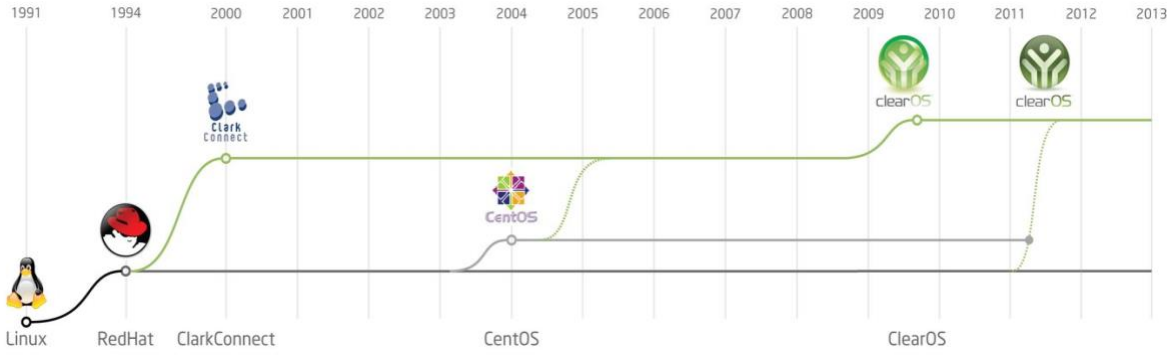
ClearOS está diseñado como un Servidor, red y puerta sistema con una elegante interfaz de usuario para su administración y este entorno está orientado para la web. ClearOS es publicado bajo la licencia GNU, tiene la libertar de descargar la imagen e instalar en PC, el código fuente es abierto en la versión Community.

ClearOS es una solución alternativa prometedora para Windows Small Business Server de Microsoft que fue terminado en 2012 (Obiniyi et al., 2012).

El progreso del desarrollo de ClearOS esta ilustrada en la figura 7.

Figura 7

Progreso de desarrollo de ClearOS



Nota. (Obiniyi et al., 2012)

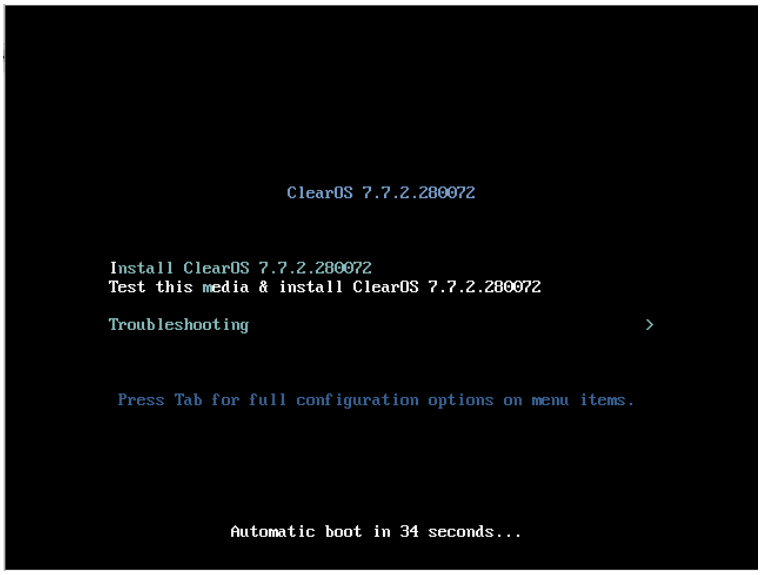
Configuración e instalación de ClearOS

Instalación

Una vez creada la USB booteable con el instalador del sistema operativo ClearOS, debe ingresar al BIOS de la placa Atomic PI, de tal manera que pueda arrancar el instalador desde la USB, cuando arranque el sistema debe mostrarse la siguiente ventana como se muestra en la siguiente figura.

Figura 8

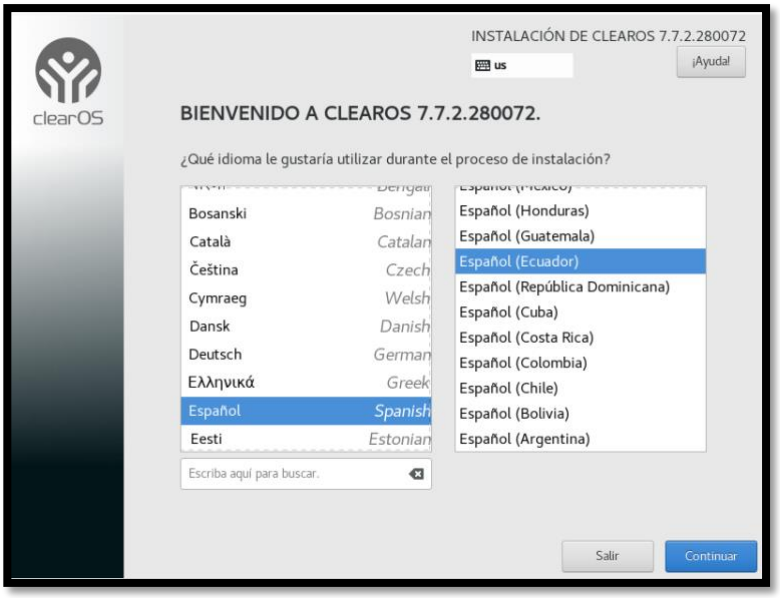
Ventana de selección para instalar ClearOS



Para proceder en la instalación se debe seleccionar el idioma de la instalación, para este caso se seleccionó idioma español y se seleccionó el español Ecuador como se muestra en la figura.

Figura 9

Ventana de selección de idioma



Luego de la selección del idioma, se debe seleccionar la ubicación de la instalación.

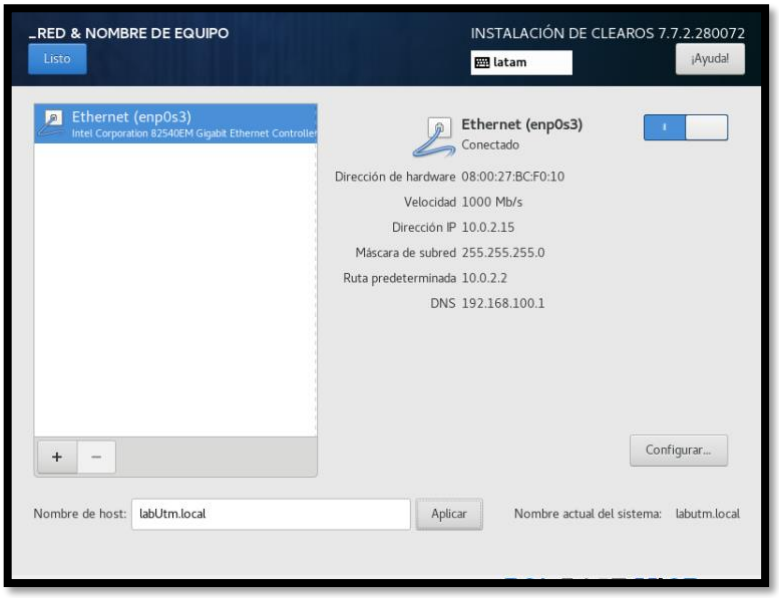
Figura 10

Ventana de selección del almacenamiento

Luego se debe dejar seleccionada la opción de Ethernet para que en cuanto se conecte a la red enseguida de reiniciar después de la instalación.

Figura 11

Configuración de la red



Una vez configurado el preinstalado, se debe dar una contraseña en la siguiente de ventana como se muestra en la figura.

Figura 12

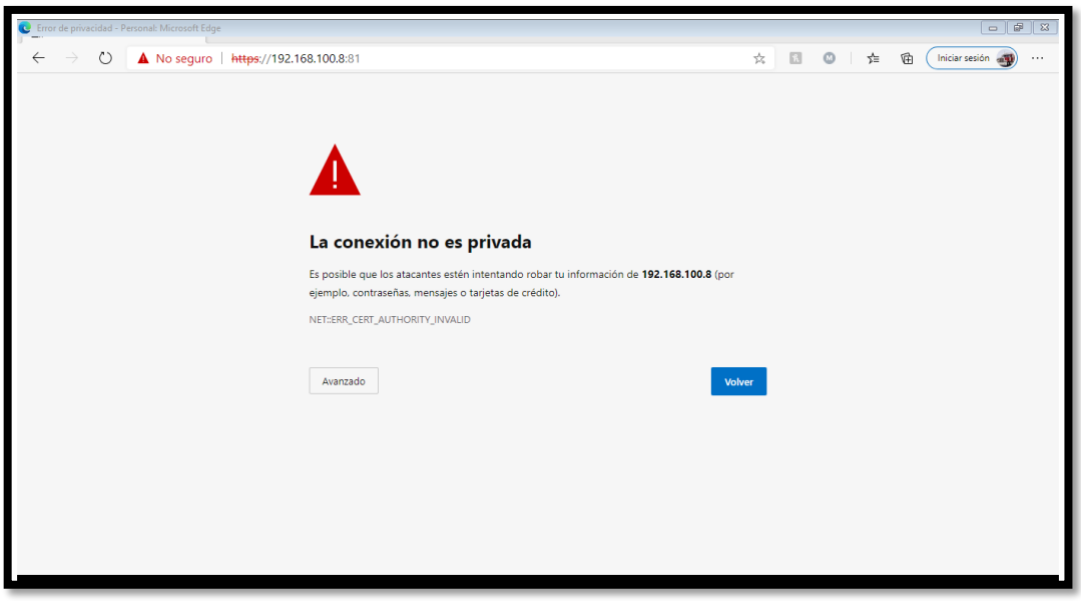
Ventana de configuración de la contraseña

Configuración

Para la configuración se debe ingresar con la dirección IP asignada desde la barra de navegación internet como se muestra en la siguiente imagen.

Figura 13

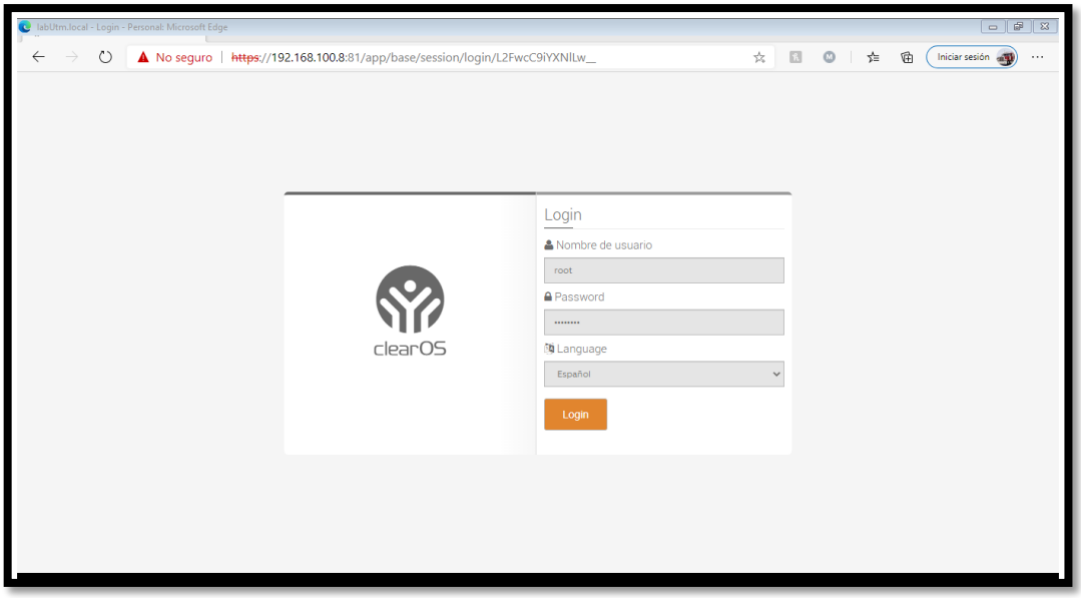
Acceso a la configuración de ClearOS



Para ingresar se debe aceptar el riesgo debido a que ClearOS no cuenta instalado con un certificado SSL aun, al continuar se deberá ingresar las credenciales antes definidas en la siguiente ventana como se muestra en la figura.

Figura 14

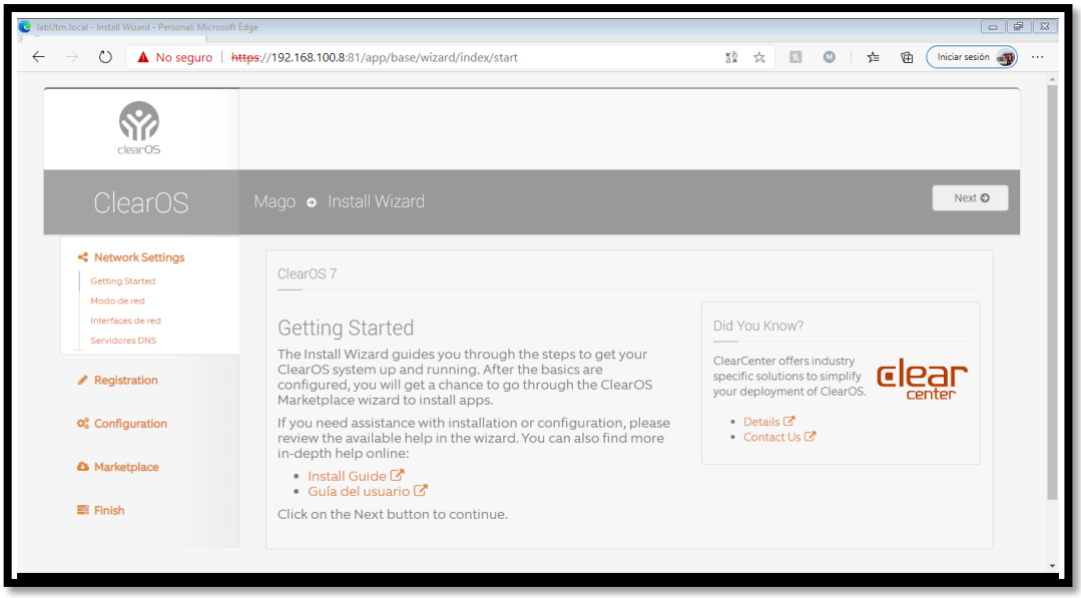
Ventana del login de ClearOS



Con las credenciales aceptadas le conducirá a la siguiente ventana principal como lo muestra en la figura.

Figura 15

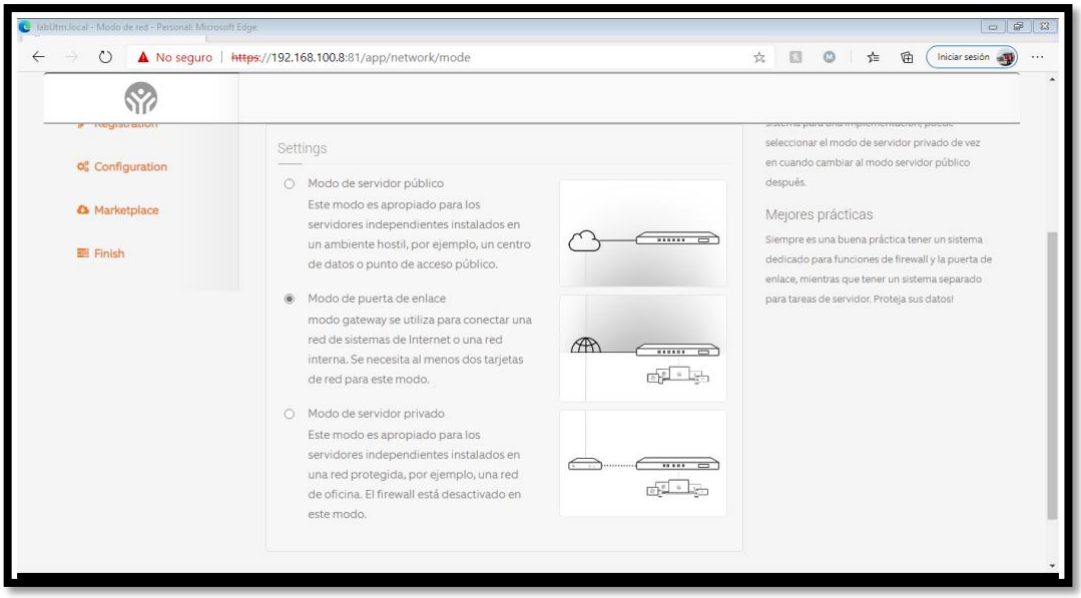
Ventana principal de ClearOS



Se debe dar clic en el botón next para continuar con la configuración así le conducirá a la siguiente ventana, en la cual se debe seleccionar el modo de la red en la cual va a funcionar el UTM, para este caso se seleccionó Modo puerta de enlace.

Figura 16

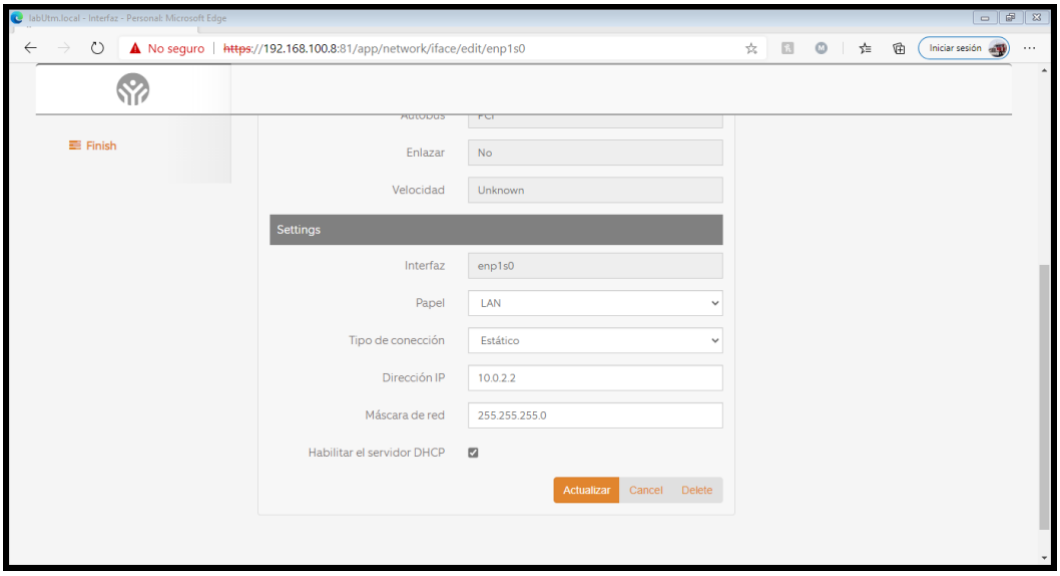
Selección del modo de red



En la siguiente ventana se debe seleccionar la interfaz de red interna y configurar la dirección IP para conexión a los dispositivos internos, como se muestra en la figura.

Figura 17

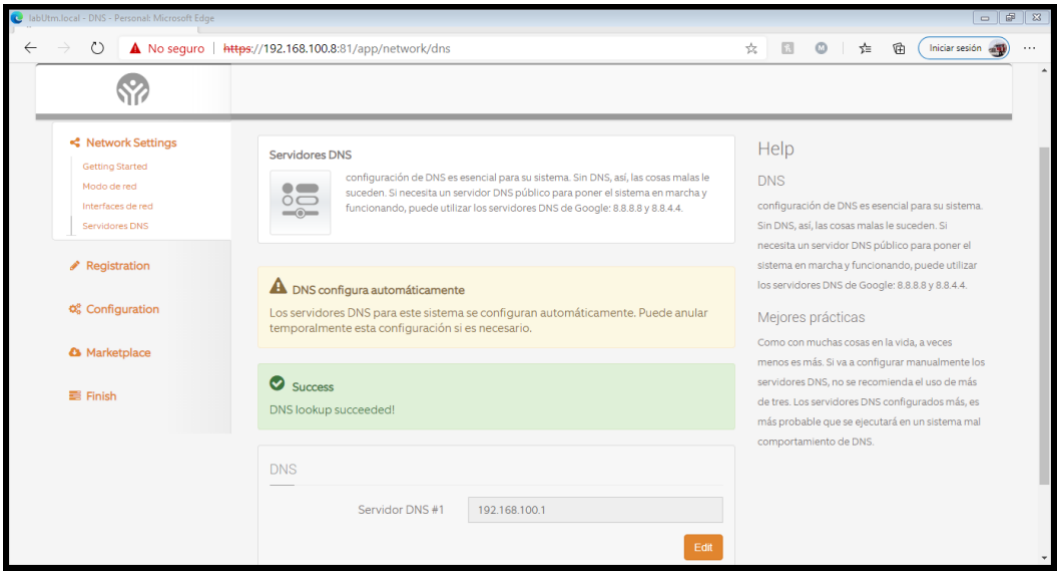
Configuración para la puerta de enlace de la red interna



En la siguiente imagen se muestra la comprobación del servidor de DNS

Figura 18

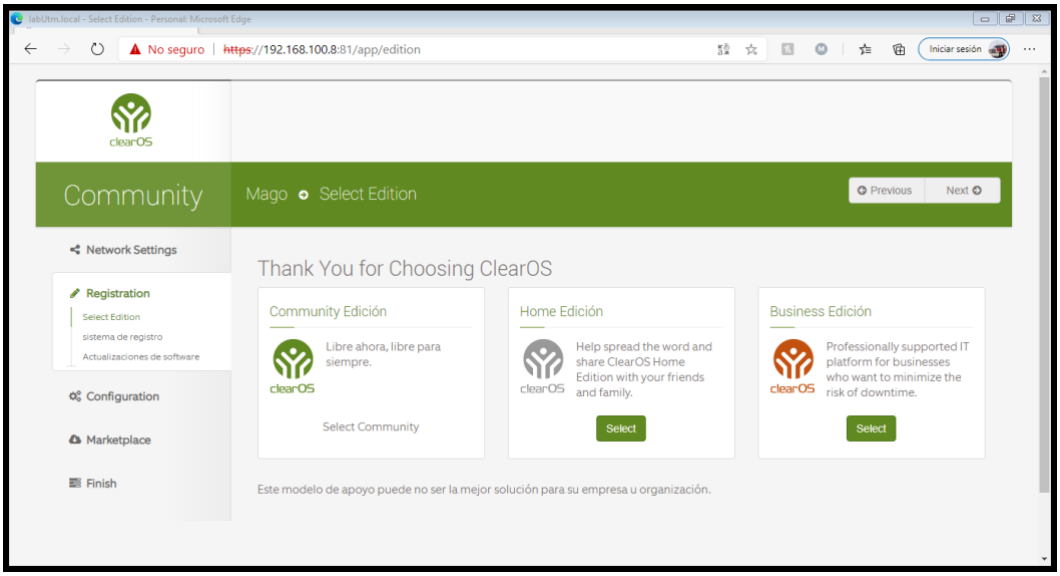
Verificación de servidor DNS



Si es verificado el servidor de DNS se puede continuar con la selección del tipo de licencia de ClearOS, para este caso de estudio se seleccionó la de Community como se ve en la figura.

Figura 19

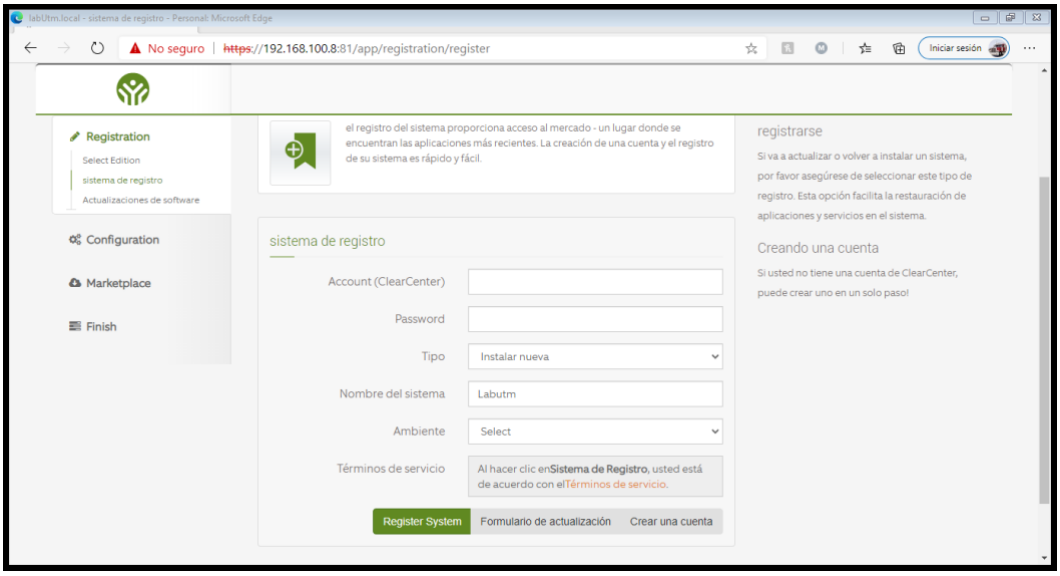
Selección del tipo de licencia



Se debe registrar la licencia para poder continuar con la instalación en el siguiente formulario como se muestra en la figura.

Figura 20

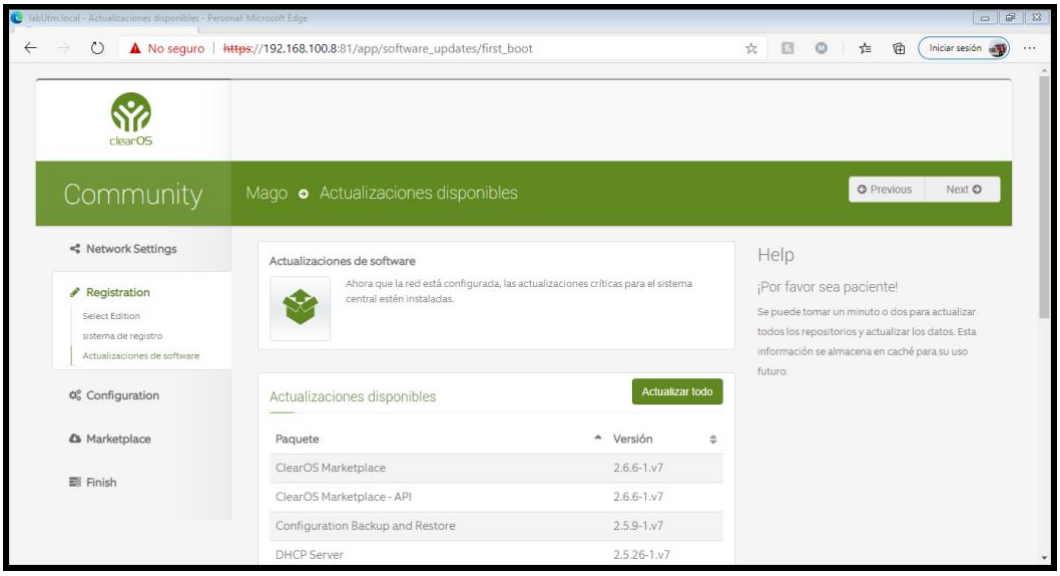
Formulario de registro de la licencia



Con el registro completo se puede continuar con la siguiente ventana de actualización de paquetes como se ve en la siguiente figura.

Figura 21

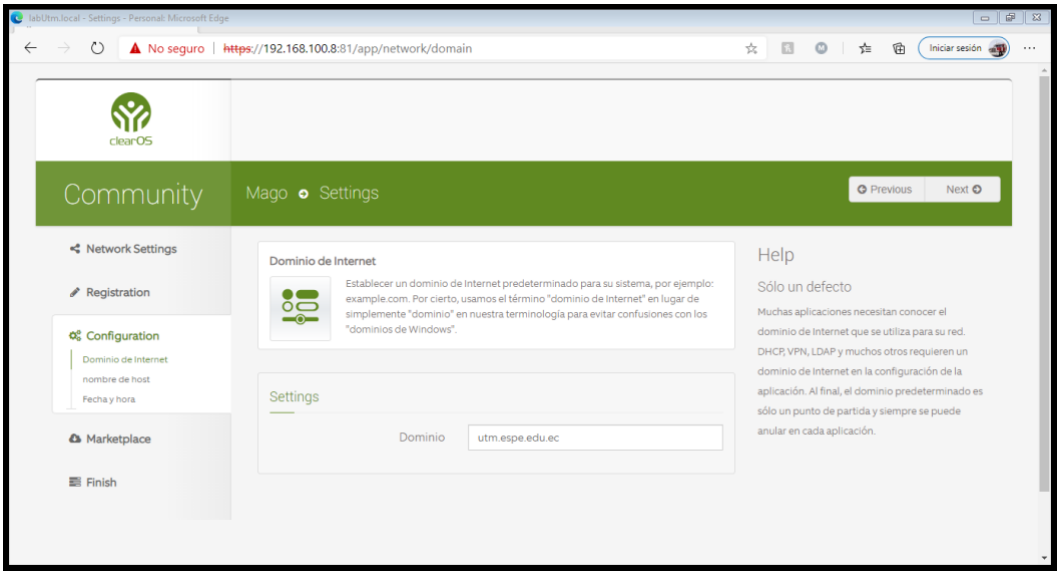
Ventana de actualización paquetes



Con los paquetes actualizados se puede continuar con la configuración, se colocó el nombre del dominio, utm.espe.edu.ec como se muestra en la siguiente figura.

Figura 22

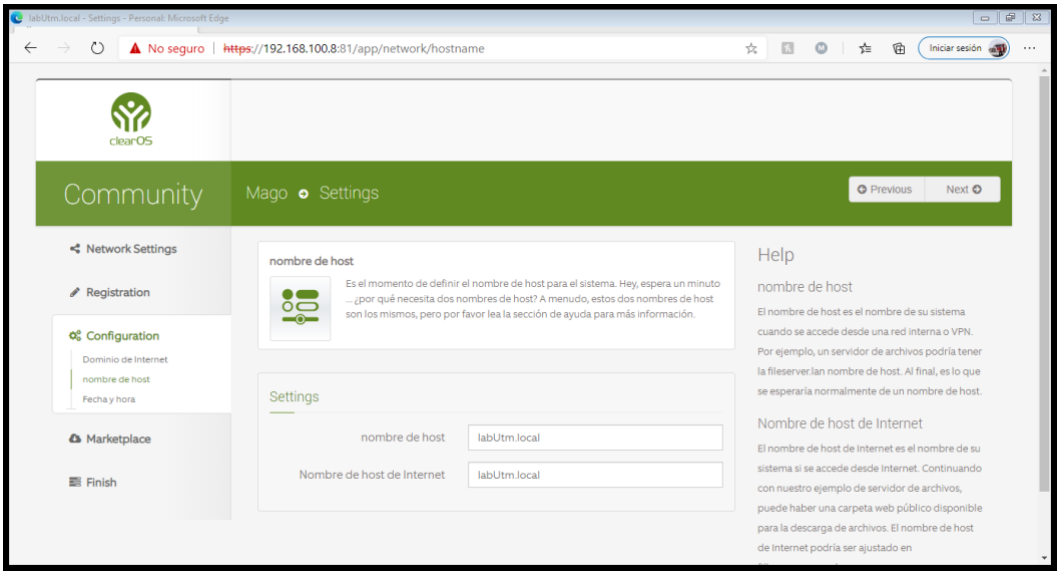
Ingreso de dominio



En la siguiente ventana se muestra el nombre del host el cual se lo coloco en la instalación, como se muestra en la siguiente figura.

Figura 23

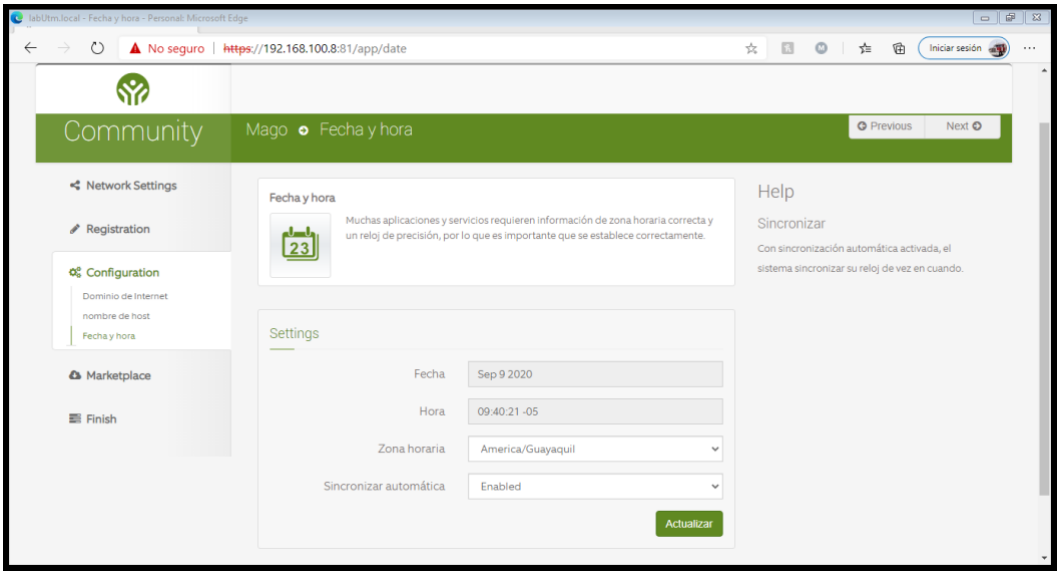
Registro del nombre del host



A continuación, se debe comprobar si la hora y fecha están adecuadamente configuradas, como en la siguiente imagen.

Figura 24

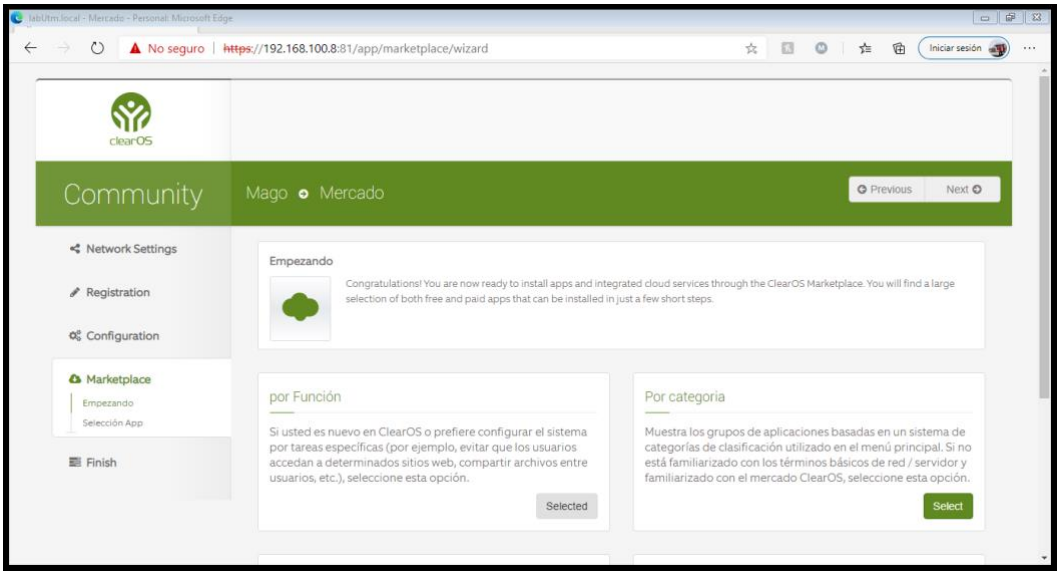
Ventana de fecha y hora



Enseguida se muestra la selección del tipo de categorías de los complementos como los va a instalar, en este caso se seleccionó por función.

Figura 25

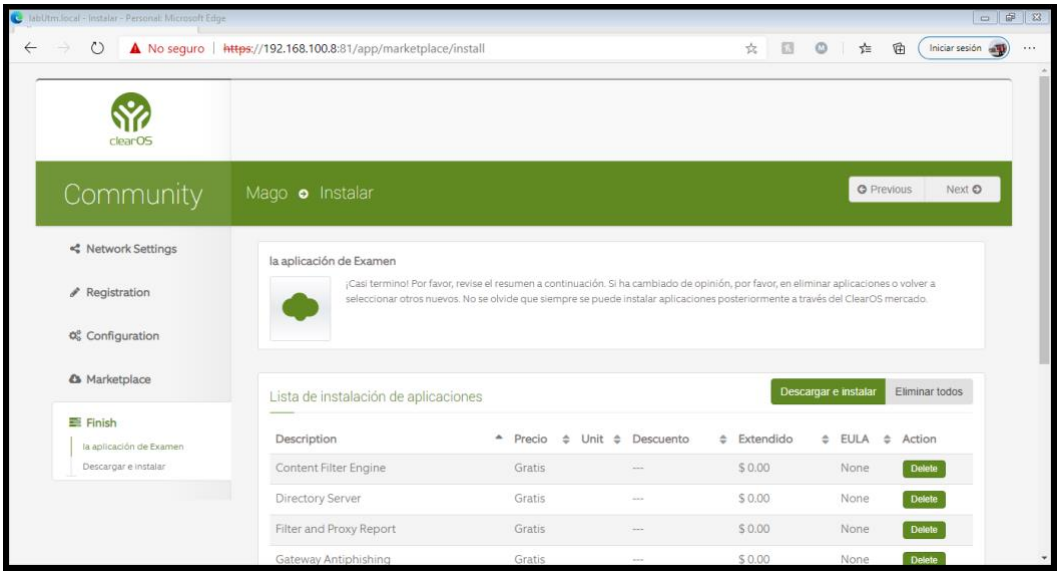
Ventana de selección de tipo de clasificación de los complementos



En la siguiente ventana se debe seleccionar los complementos para su instalación como se ve en la siguiente figura.

Figura 26

Ventana de descarga e instalación de complementos

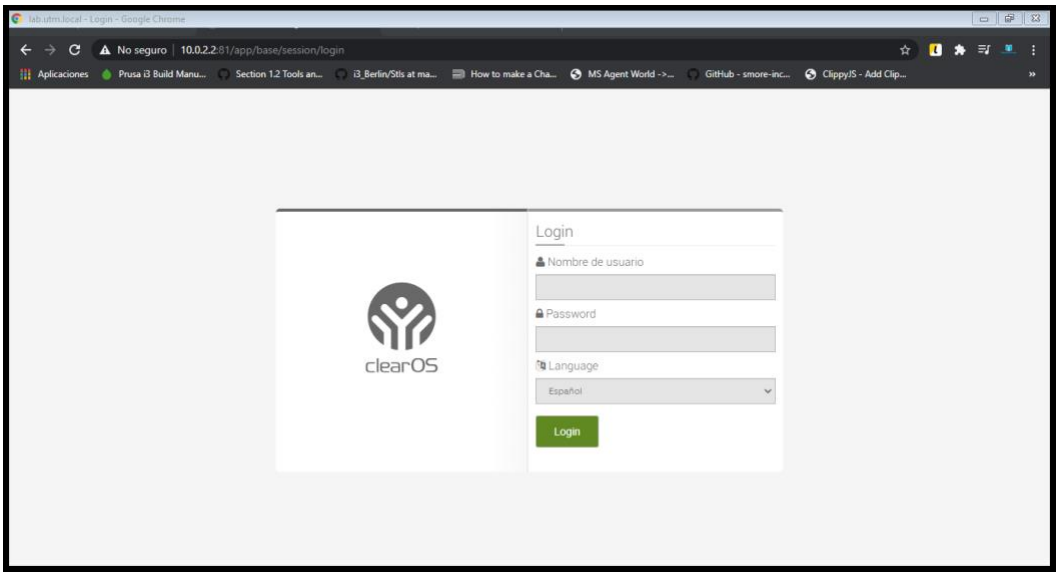


ClearOS interfaz de usuario

ClearOS cuenta con una interfaz de usuario intuitiva orientada a la Web, como a continuación se muestra en la Figura.

Figura 27

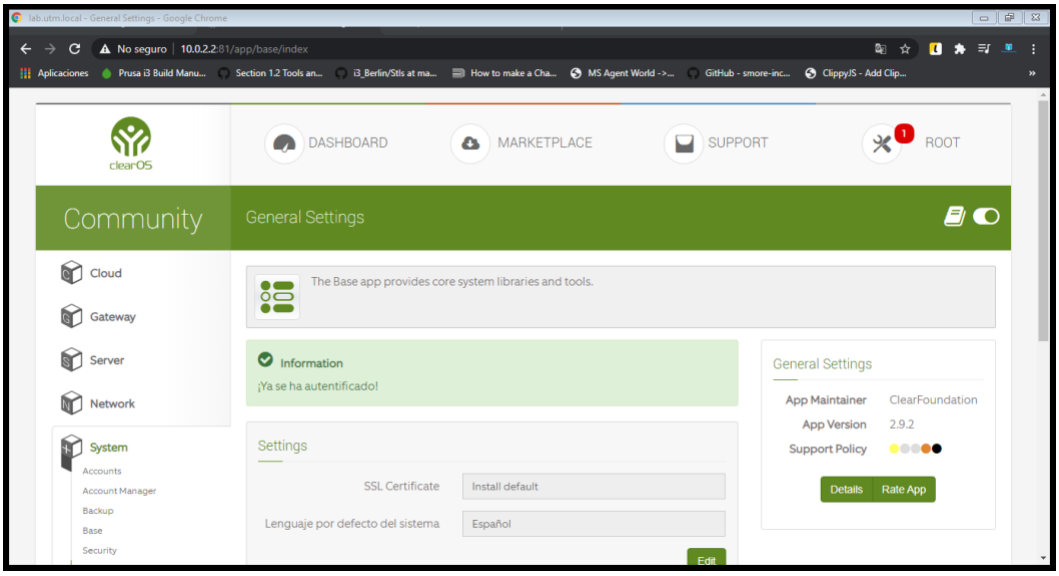
Ingreso a ClearOS



Una vez dentro de la aplicación se mostrará la siguiente pantalla donde puede encontrar las diversas opciones para interactuar con la misma, en la siguiente Figura se muestra la pantalla de administración de ClearOS.

Figura 28

Pantalla principal de ClearOS

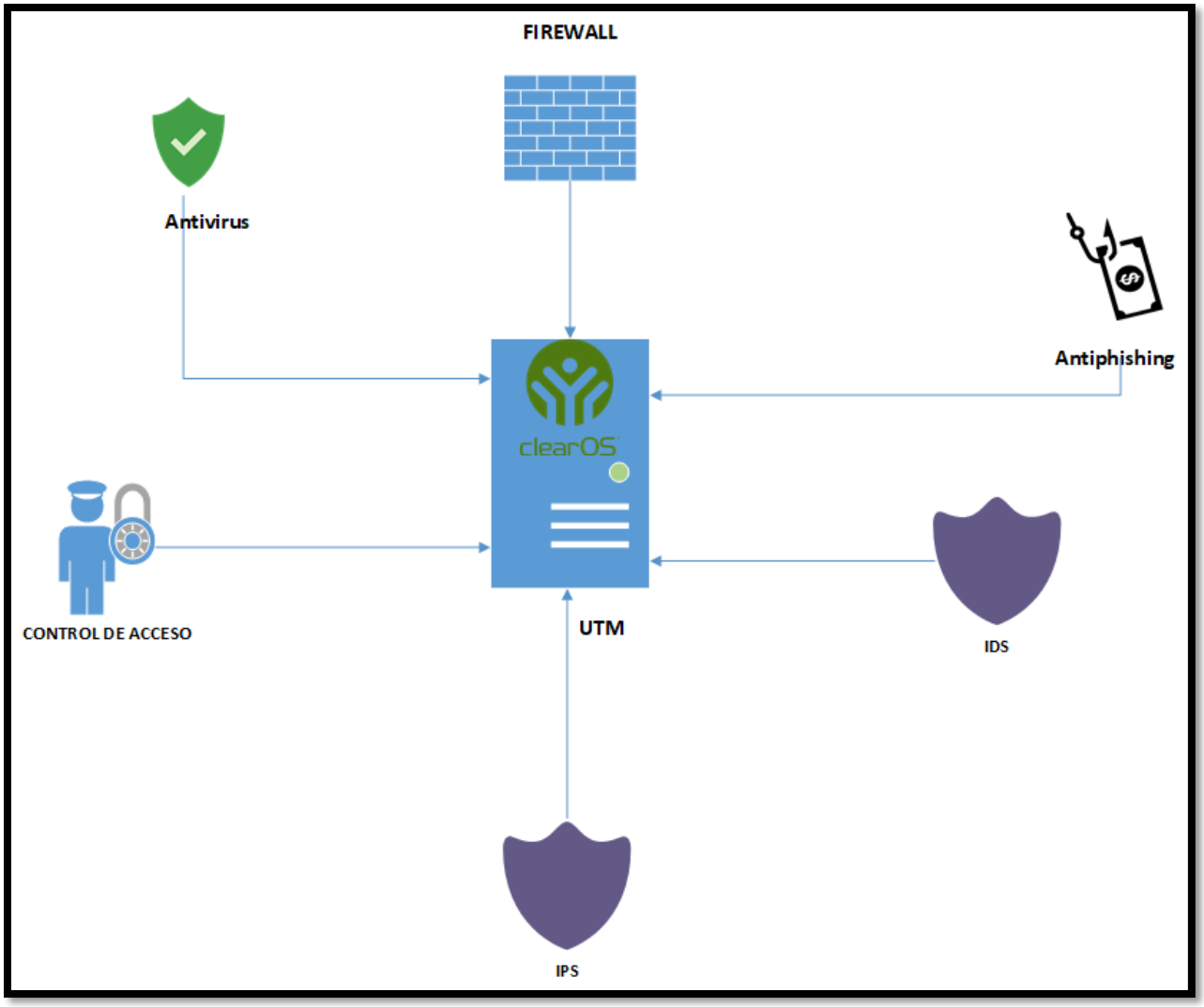


Arquitectura del UTM

En la siguiente imagen se muestra como está funcionando la arquitectura del sistema UTM.

Figura 29

Arquitectura del UTM



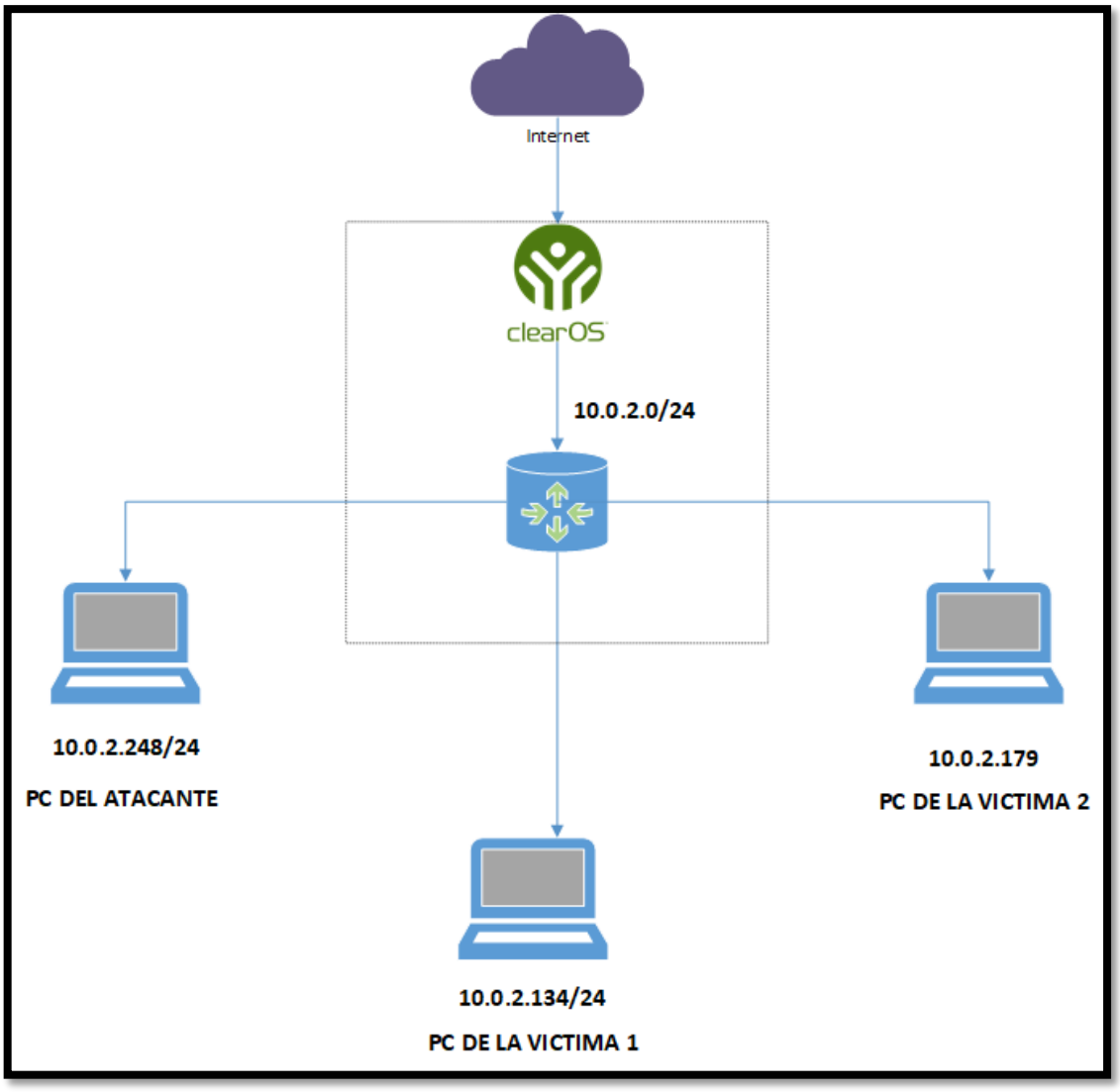
Laboratorio de pruebas

Para probar la eficacia de la implementación del sistema operativo ClearOS sobre la placa IoT Atomic Pi, para lo cual se utilizó herramientas de Pentesting instaladas sobre Kali Linux.

Estas pruebas se realizaron sobre un entrono controlado como se muestra en la siguiente figura.

Figura 30

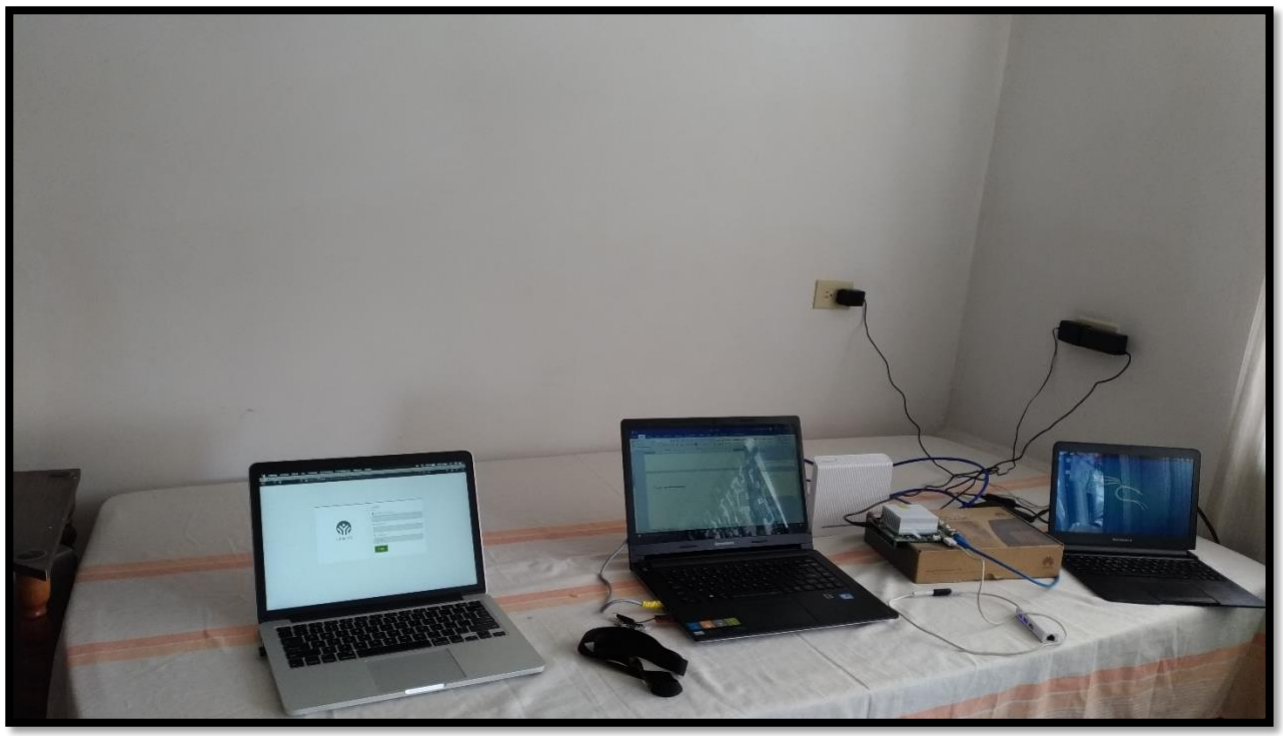
Arquitectura de la red del escenario de pruebas



En las siguientes imágenes se muestra el laboratorio implementado conforme a la arquitectura, de tal manera poder ejecutar los ataques dentro de un entorno controlado.

Figura 31

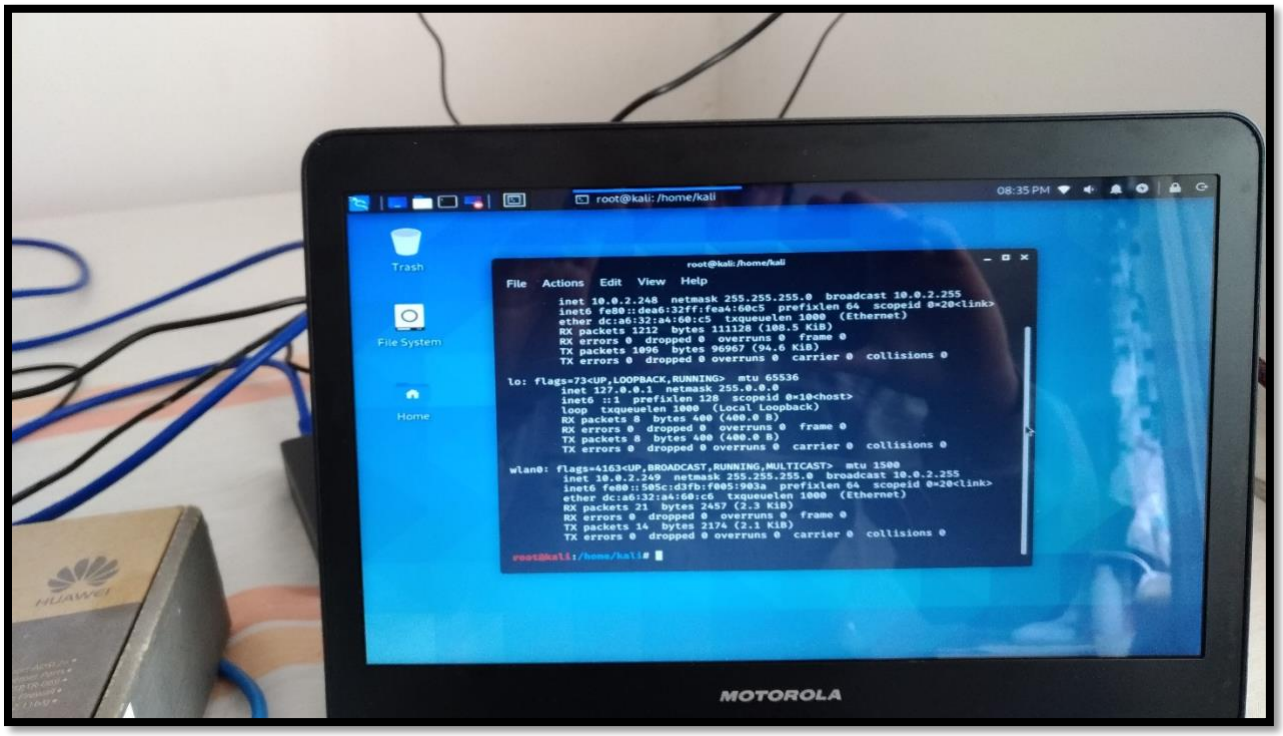
Laboratorio de pruebas



A continuación, se muestra la máquina del atacante con IP 10.0.2.248, la cual es una Raspberry Pi 4 cuenta instalada el sistema operativo Kali Linux, como se muestra en la siguiente imagen.

Figura 32

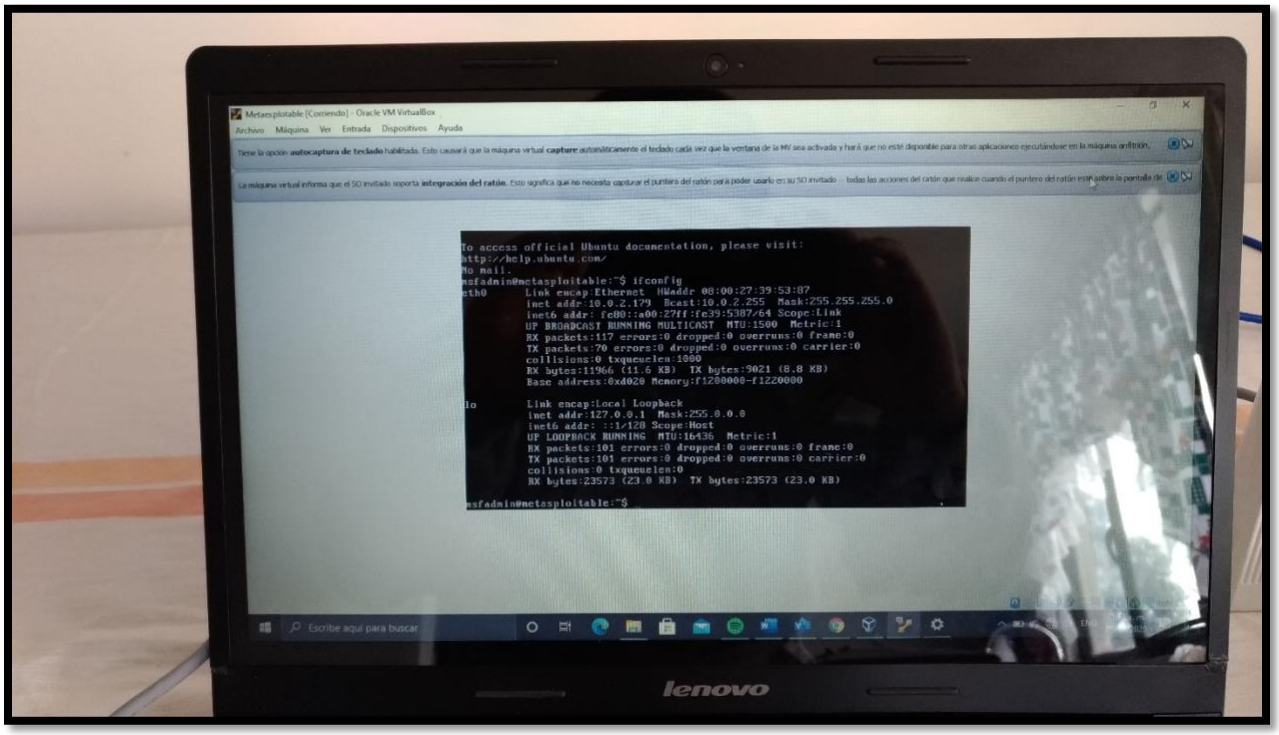
Máquina atacante



A continuación, se muestra la máquina de la víctima, la cual se instaló dentro de una máquina virtual el sistema operativo llamado Metasploitable, el cual cuanta con varias vulnerabilidades ideal para realizar las pruebas.

Figura 33

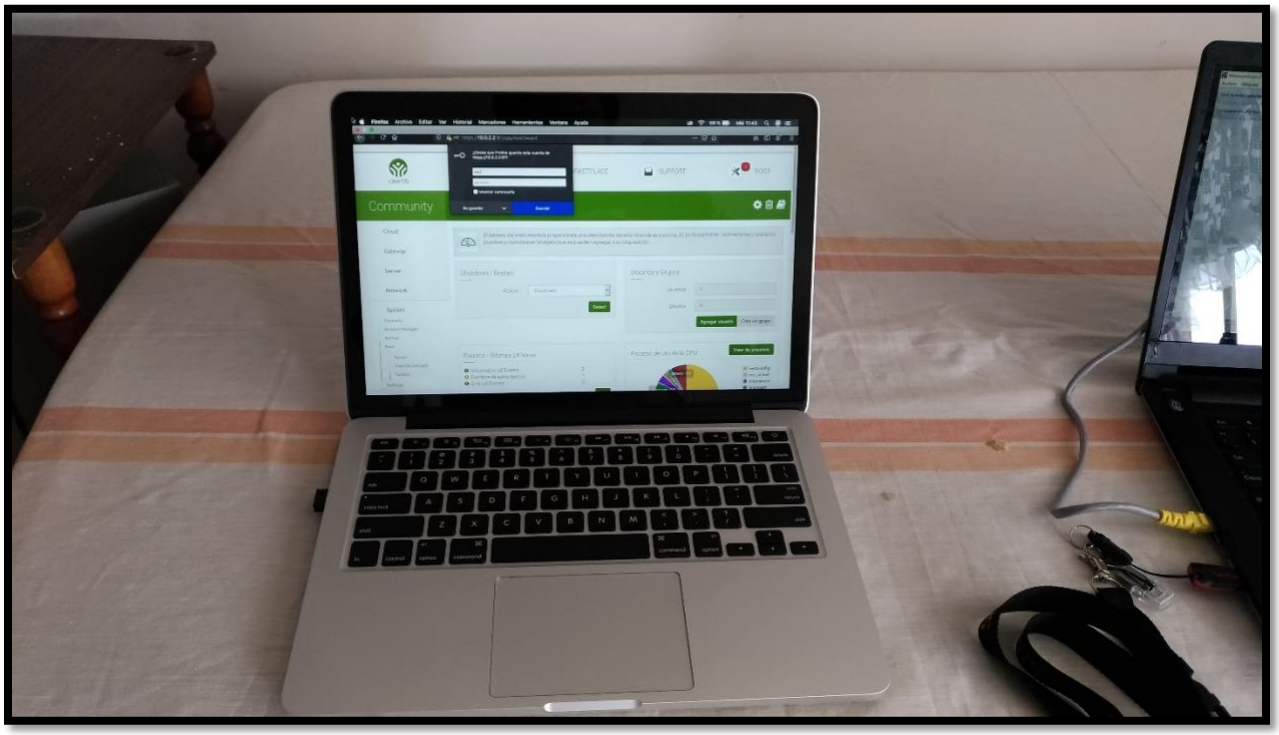
Máquina víctima



Para acceder al tablero de control del ClearOS se lo debe hacer mediante un navegador web como se muestra en la siguiente imagen.

Figura 34

Tablero de control de ClearOS



Para interconectar todos los dispositivos se utilizó un modem HG520c, en modo bridge el cual permitió la conexión tanto alámbrica como inalámbrica, además se aprecia el hardware IoT Atomic PI, el mismo que se utilizó para la implementación de las funcionalidades de UTM como se muestra en la siguiente imagen.

Figura 35

Hardware Atomic PI y Modem HG520c

Capítulo V

Pruebas y análisis de resultados

Pruebas

Las pruebas se llevaron a cabo dentro de un entorno controlado, de tal manera comprobar que la implementación de las funcionalidades de UTM sobre el dispositivo IoT, resultó efectivamente mediante pruebas con la herramienta de Pentesting, de nombre Hping3 la cual cuenta con varios tipos de ataques, para ello se realizó 4 iteraciones del ataque conocido como denegación de servicios DOS, yendo desde 1000000, 100000, 10000 y 1000 repeticiones, los cuales contaran con 100 paquetes además se esconde la IP de procedencia del ataque para estimar cuan efectiva es la respuesta por parte del IPS.

Para contabilizar estos ataques se activó el analizador de paquetes como e Wireshark, así cotejar la eficiencia de la implementación.

Validaciones

Se utilizó la herramienta Hping3 para la valoración de la respuesta por parte de la herramienta Snortsam IPS que se encuentra implementado, en el hardware IoT, las pruebas se llevaron acabo de la siguiente manera, se hizo iteraciones del ataque de Synflood con las siguientes frecuencias de 1000000, 100000, 10000 y 1000.A continuación se muestran los resultados de los ataques.

Test generado con 1000000 de veces por segundo

Comando ejecutado: hping3 -S -i u1000000 10.0.2.179 -p 80 -c 100 en la figura se muestra la captura del ataque en ejecución:

Figura 36

Ataque con 1000000 repeticiones

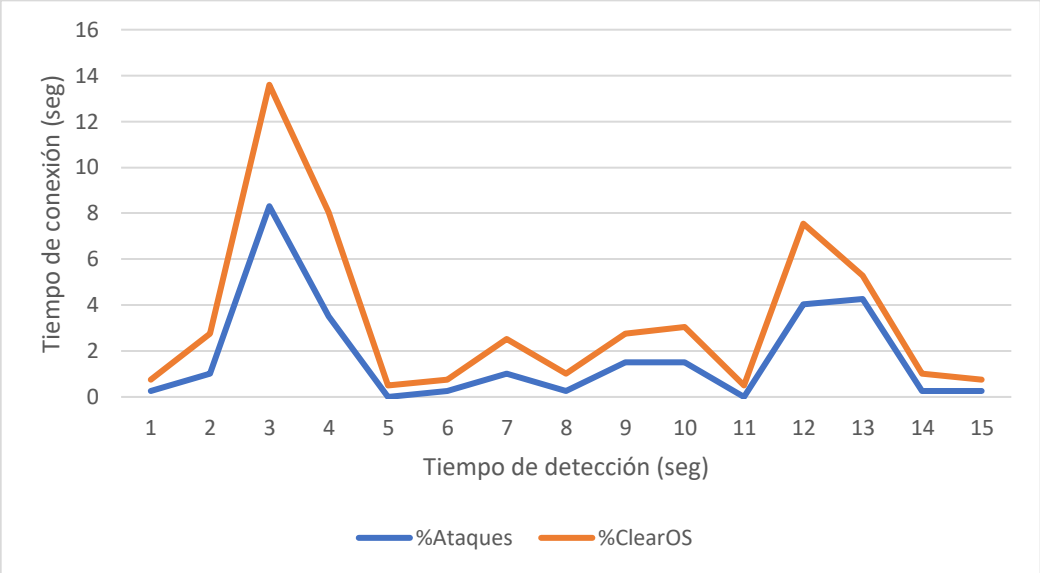
```
root@kali:/home/kali# hping3 -S -i u100000 10.0.2.134 -p 80 -c 100 >ataques
9.csv

--- 10.0.2.134 hping statistic ---
100 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

En la siguiente figura se muestra la actividad del ataque efectuado así mismo como el porcentaje del uso del ClearOS.

Figura 37

Gráfico, con un ataque de 1000000 repeticiones.



Test generado con 100000 de veces por segundo

Comando ejecutado: hping3 -S -i u100000 10.0.2.179 -p 80 -c 100 en la figura se muestra la captura del ataque en ejecución:

Figura 38

Ataque con 100000 repeticiones

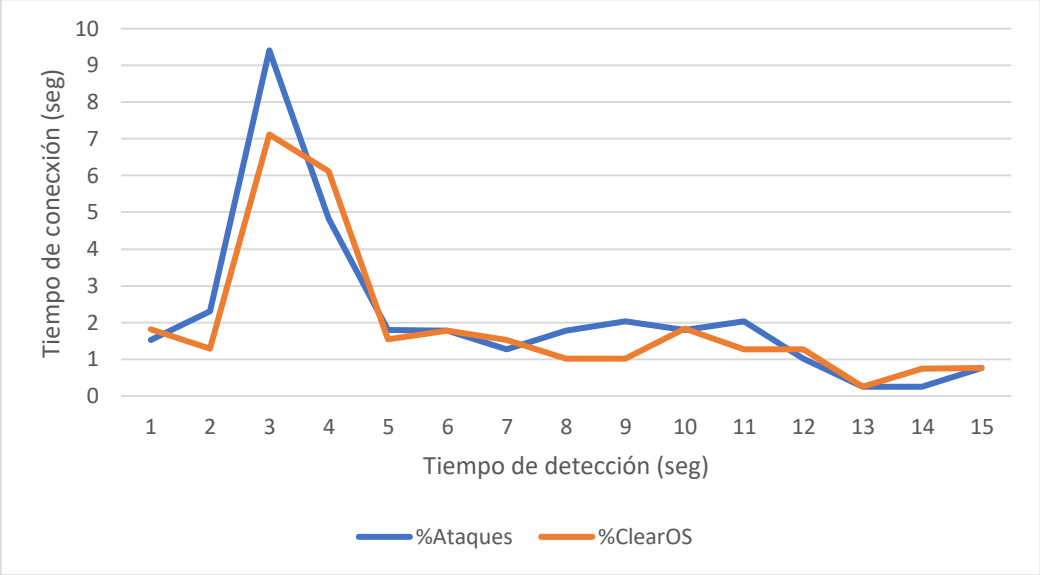
```
root@kali:/home/kali# hping3 -S -i u100000 10.0.2.134 -p 80 -c 100 >ataques
9.csv

--- 10.0.2.134 hping statistic ---
100 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

En la siguiente figura se muestra la actividad del ataque efectuado así mismo como el porcentaje del uso del ClearOS.

Figura 39

Gráfico, con un ataque de 100000 repeticiones.



Test generado con 10000 de veces por segundo

Comando ejecutado: hping3 -S -i u10000 10.0.2.179 -p 80 -c 100 en la figura se muestra la captura del ataque en ejecución:

Figura 40

Ataque con 10000 repeticiones

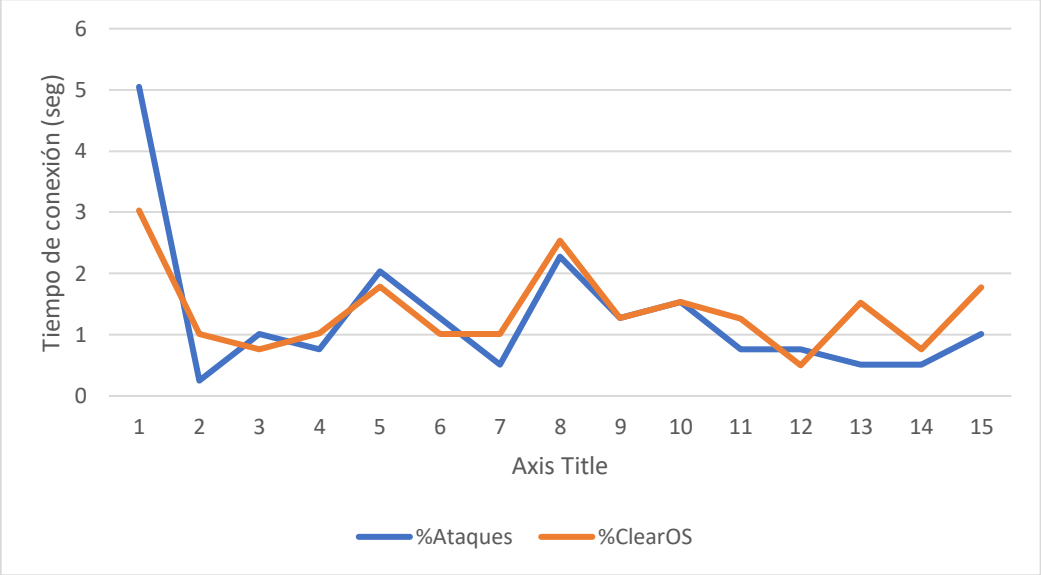
```
root@kali:/home/kali# hping3 -S -i u10000 10.0.2.134 -p 80 -c 100 >ataques1
0.csv

--- 10.0.2.134 hping statistic ---
100 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

En la siguiente figura se muestra la actividad del ataque efectuado así mismo como el porcentaje del uso del ClearOS.

Figura 41

Gráfico, con un ataque de 10000 repeticiones.



Test generado con 1000 de veces por segundo

Comando ejecutado: hping3 -S -i u1000 10.0.2.179 -p 80 -c 100 en la figura se muestra la captura del ataque en ejecución:

Figura 42

Ataque con 1000 repeticiones

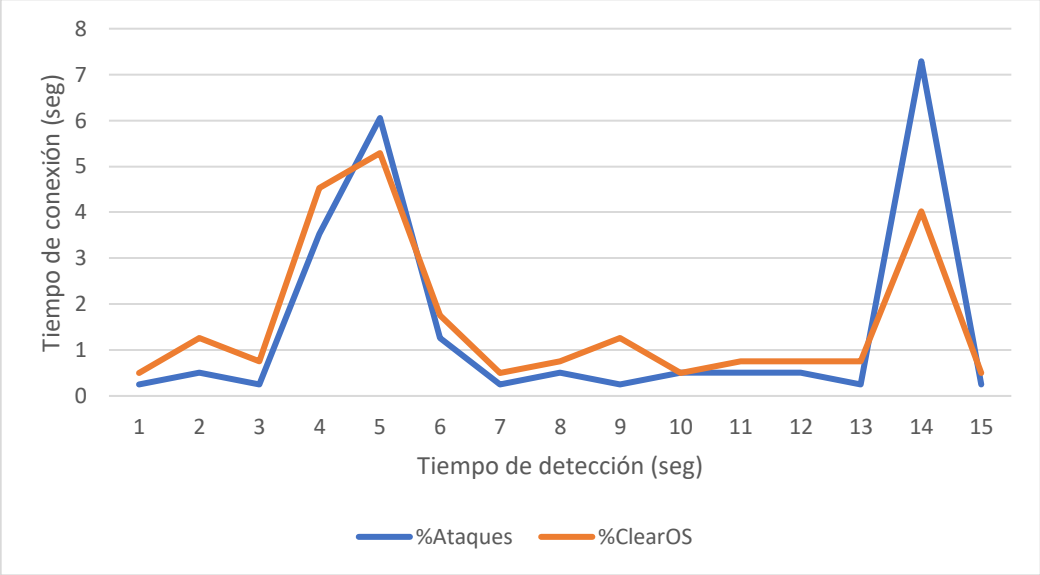
```
root@kali:/home/kali# hping3 -S -i u1000 10.0.2.134 -p 80 -c 100 >ataques11
.csv

--- 10.0.2.134 hping statistic ---
100 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

En la siguiente figura se muestra la actividad del ataque efectuado así mismo como el porcentaje del uso del ClearOS

Figura 43

Gráfico, con un ataque de 1000 repeticiones.



Resultados

Mediante la herramienta Wireshark se pudo recopilar los siguientes datos de sincronización de paquetes como se muestra en la siguiente tabla.

Tabla 5

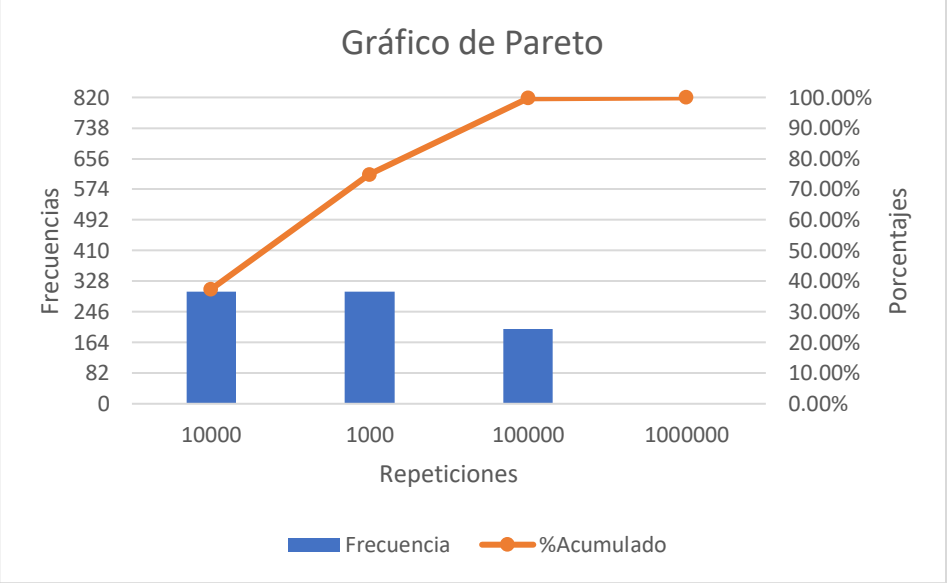
Resultado de sincronizaciones

Repeticiones	Frecuencia	%	Acumulado	%Acumulado
10000	300	37,41%	300	37,41%
1000	300	37,41%	600	74,81%
100000	200	24,94%	800	99,75%
1000000	2	0,25%	802	100,00%
TOTALES	802	100,00%		

En base de la tabla se obtuvo el diagrama de Pareto, como se muestra en la siguiente figura.

Figura 44

Diagrama de Pareto



Donde se concluye que la implementación de las funcionalidades de UTM sobre el hardware Atomic PI, es efectivo en la defensa de ataques de DoS, que sean mayores de 1000000 de repeticiones mientras tanto esto implica que puede proteger hasta 50 dispositivos debido a que se trata de una licencia educativa.

Capítulo VI

Conclusiones y recomendaciones

Conclusiones

Este estudio se realizó la revisión sistemática de literatura referente a la implementación de UTM sobre un dispositivo IoT. Sobre el tema se encontraron muy pocos trabajos. Este insumo permitió armar adecuadamente el estado del arte, fue la base para la implementación de las funcionalidades UTM sobre una placa Atomic PI.

Se realizaron varias configuraciones y adaptaciones en el sistema operativo ClearOS, el cual tiene licencia libre en su versión Community. Se utilizó esta versión con fines educativos ya que se dispone de una licencia con vigencia de 2 años.

Esta implementación de ClearOS es la adecuada para hogares y microempresas las cuales no deben contar con más de 20 empleados para su eficaz respuesta. Además, el consumo energético es el más adecuado pues su consumo es de 20 Watts lo que implica un ahorro para una empresa, sobre todo no genera altas temperaturas con ello no necesita de disponer un cuarto extra ventilado con costos altos para su construcción.

Para las pruebas de concepto se utilizó software libre para la inyección, recolección, procesamiento y análisis de tráfico, lo cual muestra que es una solución de bajo costo.

Como resultado final se logró determinar que las funcionalidades de un sistema de detección y prevención de intrusos como de filtrado de paquetes fueron exitosas.

Recomendaciones

Para la óptima implementación del UTM en su organización es recomendable configurar adecuadamente los puntos de acceso.

Si registra a un empleado en este sistema, recuerde al ser despedido también deberá ser dado de baja las credenciales de acceso debido a que el gran número de ataques se los realiza mediante los exempleados enojados los cuales de una u otra manera desean hacer daño a la organización.

Referencias bibliográficas

AMR. (2019). *Kaspersky boletín de seguridad 2019. Estadísticas | Securelist*. https://securelist.lat/kaspersky-security-bulletin-2019-statistics/89943/

Cisco Systems, I. . C. N. A. P. (2005). *Academia de Networking de Cisco Systems : fundamentos de seguridad de redes : especialista en Firewall Cisco* (1a ed.). Cisco Systems;Pearson Educacio

Colmenares, M., & E., A. (2017). Investigación-acción participativa: una metodología integradora del conocimiento y la acción. *Revista Latinoamericana de Educación*, *3*(1), 102–115.

Duarte, E. S. (2008). *LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC) DESDE UNA PERSPECTIVA SOCIAL*. *XII*, 155–162.

EL COMERCIO. (2019). *Ecuador denuncia 40 millones de ciberataques tras retiro de asilo a Assange | El Comercio*. https://www.elcomercio.com/actualidad/ecuador-denuncia-millones-ciberataques-assange.html

Flores, D., González, L., & Becerra, B. (2012). Objetos de aprendizaje: Una Investigación Bibliográfica y Compilación Learning Objects: A Literature Research and Compilation. In *Revista de Educación a Distancia (RED)* (Issue 34). http://www.um.es/ead/red/34

Fuertes, W., Zambrano, P., Sánchez, M., Santillán, M., Villacís, C., Toulkeridis, T., & Torres, E. (2014). Repowering an Open Source Firewall Based on a Quantitative Evaluation. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 14, Issue 11).

Gummadi, S., & Shanmugasundaram, R. (2012). Effective utilization of multicore processor for unified threat management functions. *Journal of Computer Science*, *8*(1), 68–75. https://doi.org/10.3844/jcssp.2012.68.75

Hu, H. (2015). *Improving Unified Threat Management Architecture Based on Net Channel*

Technology. *Icemct*, 1469–1472. https://doi.org/10.2991/icemct-15.2015.308

Iso27000.es. (2005). *Serie 27k*. https://www.iso27000.es/iso27000.html

Kaspersky. (2019). *¿Qué es la gestión unificada de amenazas (UTM)? | Definición de UTM | Kaspersky*. https://latam.kaspersky.com/resource-center/definitions/utm

Kyaw, A. K., Chen, Y., & Joseph, J. (2016). Pi-IDS: Evaluation of open-source intrusion detection systems on Raspberry Pi 2. *2015 2nd International Conference on Information Security and Cyber Forensics, InfoSec 2015*, 165–170. https://doi.org/10.1109/InfoSec.2015.7435523

Manuti. (2019). *Sobre la Atomic Pi - Raspberry para torpes*. https://raspberryparatorpes.net/rivales/sobre-la-atomic-pi/

Obiniyi, A. A., Absalom, E. E., & Dikko, M. (2012). Network Security and Firewall Technology. *International Journal of Dependable and Trustworthy Information Systems*, *2*(2), 40–60. https://doi.org/10.4018/jdtis.2011040103

Pareja, S. (2017). *Implementación de un Firewall construido a partir de software y una placa de circuitos compacta o SBC (Single Board Computer) en la empresa TAIO Systems de la ciudad de Popayán.* Universidad Nacional Abierta y a Distancia UNAD. http://repository.unad.edu.co/handle/10596/17389

Ramírez, M., & Jiménez, F. (2016). *ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA ESCUELA DE INGENIERÍA ELECTRÓNICA EN*. Escuela Superior Politécnica de Chimborazo. http://dspace.espoch.edu.ec/handle/123456789/5453

Rehman, R. U. (2003). *Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort ... - Rafeeq Ur Rehman - Google Libros*. Prentice Hall. https://books.google.com.ec/books?hl=es&lr=&id=1WKrLbh23LAC&oi=fnd&pg=PA1&dq=Intrusion+Detection+Systems+Rehman&ots=5r144dSHdx&sig=-

k5KtltGhXsA5WhMECiBGAyAEkU&redir_esc=y#v=onepage&q=Intrusion Detection Systems Rehman&f=false

Sanfilippo, S. (2020). *Hping - Active Network Security Tool*. http://www.hping.org/

Tam, K., Salvador, M. H. H., McAlpine, K., Basile, R., Matsugu, B., & More, J. (2012). UTM Security with Fortinet: Mastering FortiOS. In *UTM Security with Fortinet: Mastering FortiOS*. Elsevier Inc. https://doi.org/10.1016/C2011-0-05893-3

VMware. (2020). *What is Application Security? | VMware Glossary*. https://www.vmware.com/topics/glossary/content/application-security

Wireshark. (2020). *Wireshark · Go Deep.* https://www.wireshark.org/