UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO.

FACULTAD DE CIENCIAS DE LA INGENIERÍA.

CARRERA INGENIERÍA EN TELEMÁTICA

Proyecto de investigación
previo a la obtención del título
Ingeniero en Telemática.

Título Del Proyecto De Investigación:

"ANÁLISIS DINÁMICO DE MALWARE EN AMBIENTE DE RED CORPORATIVO VIRTUALIZADO"

Autor:

Orlando Jesús Brito Casanova.

Director de Proyecto de Investigación:

Ing. Emilio Rodrigo Zhuma Mera, MsC.

Quevedo – Los Ríos - Ecuador

2018

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

Yo, ***Orlando Jesús Brito Casanova,*** con C.I. ***1206815712,*** declaro que la investigación aquí descrita es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Técnica Estatal de Quevedo, puede hacer uso de los derechos correspondientes a este documento, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

.....

BRITO CASANOVA ORLANDO JESÚS
C.C.No. 1206815712
CEL. 0981121556
orlando.brito2013@uteq.edu.ec
AUSPICIANTE

CERTIFICACIÓN DE CULMINACIÓN DEL PROYECTO DE INVESTIGACIÓN

El suscrito, ***Ing. Emilio Rodrigo Zhuma Mera***, Docente de la Universidad Técnica Estatal de Quevedo, certifica que el estudiante ***Orlando Jesús Brito Casanova***, realizó el Proyecto de Investigación de grado titulado ***"Análisis dinámico de malware en ambiente de red corporativo virtualizado"***, previo a la obtención del título de ***Ingeniero en Telemática***, bajo mi dirección, habiendo cumplido con las disposiciones reglamentarias establecidas para el efecto.

Ing. Zhuma Mera Emilio Rodrigo

DIRECTOR DE PROYECTO DE INVESTIGACIÓN

CERTIFICADO DEL REPORTE DE LA HERRAMIENTA DE PREVENCION DE COINCIDENCIA Y/O PLAGIO ACADÉMICO

Yo, Ing. Zhuma Mera Emilio, MsC, en calidad de Director del Proyecto de Investigación titulado: **"ANÁLISIS DINÁMICO DE MALWARE EN AMBIENTE DE RED CORPORATIVO VIRTUALIZADO",** me permito manifestar a usted y por medio del Consejo Académico de Facultad lo siguiente:

Que, el estudiante: BRITO CASANOVA ORLANDO JESÚS, egresados de la Facultad Ciencias de la Ingeniería, ha cumplido con las correcciones pertinentes e ingresado su Proyecto de Investigación al sistema URKUND, por lo que tengo a bien certificar la siguiente información sobre el informe del sistema anti plagio con un porcentaje de 2%

URKUND

Documento	BritoCasanovaOrlando.Jesus_Telematica_AnalisisDinamicoDeMalware.docx (D42823339)
Presentado	2018-10-21 02:31 (-05:00)
Presentado por	orlando.brito2013@uteq.edu.ec
Recibido	ezhuma.uteq@analysis.urkund.com
Mensaje	Brito Casanova Orlando Jesus - Análisis dinámico de malware en ambiente de red corporativo virtualiz Mostrar el mensaje completo
	2% de estas 52 páginas, se componen de texto presente en 10 fuentes.

Ing. Emilio Zhuma Mera, MsC.

DIRECTOR DE PROYECTO DE INVESTIGACION

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA INGENIERÍA

CARRERA INGENIERÍA EN TELEMÁTICA

PROYECTO DE INVESTIGACIÓN

Título:

"ANÁLISIS DINÁMICO DE MALWARE EN AMBIENTE DE RED CORPORATIVO VIRTUALIZADO"

Presentado a la Comisión Académica como requisito previo a la obtención del título de Ingeniero en Telemática.

Aprobado por:

PRESIDENTE DEL TRIBUNAL
ING. JANETH MORA SECAIRA, PhD

MIEMBRO DEL TRIBUNAL
ING. FABRICIO MARCILLO VERA Msc.

MIEMBRO DEL TRIBUNAL
ING. JOSÉ TUBAY VERGARA Msc.

QUEVEDO – LOS RÍOS - ECUADOR
2018

CERTIFICACIÓN DE REDACCIÓN TÉCNICA DEL PROYECTO DE INVESTIGACIÓN

La suscrita **Lcda. Verónica Osorio Sánchez, MSc,** docente de la Universidad Técnica Estatal de Quevedo, certifica que el Brito Casanova Orlando Jesús, realizó el Proyecto de Investigación de Grado Titulado **"ANÁLISIS DINÁMICO DE MALWARE EN AMBIENTE DE RED CORPORATIVO VIRTUALIZADO"**, previo a la obtención del título de **INGENIERO EN TELÉMATICA,** bajo mi dirección, habiendo cumplido con las disposiciones reglamentarias establecidas para el efecto.

.....

Lcda. Verónica Osorio Sánchez, MSc, MSc

RESPONSABLE DE REDACCIÓN TÉCNICA

Agradecimiento

La universidad como centro de enseñanza me ha otorgado valiosos conocimientos académicos y de vida, terminando de forjar el carácter de un guerrero predispuesto para grandes retos, agradezco a todos los docentes con quienes tuve la oportunidad de compartir y a mis compañeros de clases quienes se convirtieron en familia, enseñándome el valor del trabajo de equipo y que no importa que tan difícil sea el desafío, con cabeza fría y compañerismo todo puede ser superado.

Una guía correcta es imprescindible para el alcance de objetivos, agradezco a mis tutores Ing. Paulo Esteban Chiliguano Torres (hasta el 30 de Septiembre del 2018) e Ing. Emilio Rodrigo Zhuma Mera (Presente), por la ayuda prestada en cuanto a la investigación y al correcto encaminamiento del proyecto.

La familia es el cimiento de la sociedad, un brazo fuerte ante turbulentas tormentas, agradezco a mis padres Ing. Ángel Orlando Brito Ávila y Sra. Yolanda del Carmen Casanova Intriago por los valores morales enseñados con el ejemplo, y a mis hermanos Thalía, Gema, Celia y Geovanny por su compañía incondicional y comprensión.

El valor de la amistad no es medible, excede la comprensión humana, por ello agradezco con toda el alma a mi mejor amiga Linda Thalía Huacón Salazar, por ser un ángel en mi vida, por su escucha, motivación y contribución para mi auto superación, espiritual y emocional, agradezco a la vida por cruzar nuestros caminos.

Orlando Jesús Brito Casanova

Dedicatoria

A todos los jóvenes entusiastas de la tecnología
cuyo principal objetivo sea contribuir a la
sociedad y al desarrollo del Ecuador.

Resumen ejecutivo y palabras claves.

La presente Investigación estudia la viabilidad de entornos corporativos virtuales para la realización de análisis dinámico de malware, características y facilidades ofertadas por el sistema hipervisor «Proxmox» y el empleo de tecnología de virtualización «LXC» y «KVM» para el aseguramiento de la operatividad y el correcto aislamiento de los componentes con muestras reales a ejecutar. Se propone una topología modesta de seguridad perimetral de amplio uso empleando una DMZ con cortafuego en trípode, red interna y añadiendo una red de monitoreo, como representación de ambiente empresarial a nivel pequeño, mediano o sucursal de grandes corporaciones para la abstracción en elementos mínimos permisibles a virtualizar con el menor impacto en la funcionalidad del sistema y salvaguardando el consumo de recursos físicos requeridos. Según características de zonas con gran importancia dentro de una organización (red interna y DMZ), son asechadas por código maliciosos clasificados de acuerdo al alcance esperado: masivos y dirigidos. Los elementos dentro de una Intranet con sistemas operativos populares, suelen verse mayormente vulnerados por malware masivo, con la única intención de causar perjuicios a mayor cantidad de sistemas posibles. La componente DMZ, ofrece servicios empresariales, soportada en plataformas con enfoque corporativo, principal objetivo de malware dirigido expresamente desarrollado para violentar características intrínsecas de la red o sistema víctima. El uso de herramientas externas para el desarrollo y obtención de datos necesarios sobre el comportamiento del sistema infectado y el desenvolvimiento del espécimen en ejecución con servicios como «Zabbix» y «Moloch» poseen limitaciones influyentes en la precisión del análisis dinámico y la consecuencia formulación de conclusiones y elaboración de «indicadores de compromisos» o firmas que ayuden a la detección de software maligno.

Palabras claves:

Virtualización, Análisis dinámico de malware, ambiente corporativo, KVM, LXC, Proxmox, Análisis automático, Hipervisor, Virtualización de entornos, malware dirigido y masivo.

Abstract and keywords.

This research studies the feasibility of virtual corporate environments for conducting dynamic malware analysis, features and facilities offered by the system hypervisor «Proxmox» and the use of virtualization technology «LXC» and « KVM» for the operation assurance and the correct isolation of the components with actual samples to execute. It proposes a modest and popular perimeter security topology's using a DMZ with firewall on tripod, internal network and adding a monitoring network, as a representation of business environment at small, medium level or large corporation subsidiaries to abstraction in minimum permissible elements to virtualize with the least impact on the functionality of the system and safeguarding the consumption of required physical resources. According to characteristics of áreas of great importance into an organization (internal network and DMZ), they are assented by malicious code classified according to their expected scope: massive and directed; The elements within an Intranet, with popular operating systems, are usually mostly violated by mass malware, with the only intention of causing harm to a greater number of possible systems; The DMZ component, provides enterprise services, supported on platforms with corporate focus, targeted malware specifically developed to violate intrinsic characteristics of the network or victim system. The use of external tools to develop and obtain necessary data on the behavior of the infected system and the development of the executing specimen with services such as "Zabbix" and "Moloch" have influential limitations on the accuracy of the Dynamic analysis and the resulting formulation of conclusions and elaboration of "commitments indicators" or signatures that help the detection of malignant software.

Keywords:

Virtualization, malware's dynamic analysis, enterprise network, KVM, LXC, Proxmox, Automatic Analysis, Hypervisor, environment virtualization, mass and targered malware.

Tabla de contenido

Índice de tablas

Índice de ilustraciones

Índice de anexos

Código Dublin

Título:	Análisis dinámico de malware en ambiente de red corporativo virtualizado.				
Autor:	Brito Casanova Orlando Jesús				
Palabras Claves:	Análisis dinámico	Malware masivo	Malware dirigido	Virtualización	KVM
	Ambiente corporativo	Proxmox	Hipervisor	Análisis Automático	LXC
Fecha de publicación:	3 de Diciembre del 2018				
Editorial:	Universidad Técnica Estatal de Quevedo				
Resumen:	Resumen.- La presente Investigación estudia la viabilidad de entornos corporativos virtuales para la realización de análisis dinámico de malware, características y facilidades ofertadas por el sistema hipervisor «Proxmox» y el empleo de tecnología de virtualización «LXC» y «KVM» para el aseguramiento de la operatividad y el correcto aislamiento de los componentes con muestras reales a ejecutar. Se propone una topología modesta de seguridad perimetral de amplio uso empleando una DMZ con cortafuego en trípode, red interna y añadiendo una red de monitoreo, como representación de ambiente empresarial a nivel pequeño, mediano o sucursal de grandes corporaciones para la abstracción en elementos mínimos permisibles a virtualizar con el menor impacto en la funcionalidad del sistema y salvaguardando el consumo de recursos físicos requeridos. Según características de zonas con gran importancia dentro de una organización (red interna y DMZ), son asechadas por código maliciosos clasificados de acuerdo al alcance esperado: masivos y dirigidos. Los elementos dentro de una Intranet con sistemas operativos populares, suelen verse mayormente vulnerados por malware masivo, con la única intención de causar perjuicios a mayor cantidad de sistemas posibles. La componente DMZ, ofrece servicios empresariales, soportada en plataformas con enfoque corporativo, principal objetivo de malware dirigido expresamente desarrollado para violentar características intrínsecas de la red o sistema víctima. El uso de herramientas externas para el desarrollo y obtención de datos necesarios sobre el comportamiento del sistema infectado y el desenvolvimiento del espécimen en ejecución con servicios como «Zabbix» y «Moloch» poseen limitaciones influyentes en la precisión del análisis dinámico y la consecuencia formulación de conclusiones y elaboración de «indicadores de compromisos» o firmas que ayuden a la detección de software maligno.				

	Abstract.- This research studies the feasibility of virtual corporate environments for conducting dynamic malware analysis, features and facilities offered by the system hypervisor «Proxmox» and the use of virtualization technology «LXC» and « KVM» for the operation assurance and the correct isolation of the components with actual samples to execute. It proposes a modest and popular perimeter security topology's using a DMZ with firewall on tripod, internal network and adding a monitoring network, as a representation of business environment at small, medium level or large corporation subsidiaries to abstraction in minimum permissible elements to virtualize with the least impact on the functionality of the system and safeguarding the consumption of required physical resources. According to characteristics of áreas of great importance into an organization (internal network and DMZ), they are assented by malicious code classified according to their expected scope: massive and directed; The elements within an Intranet, with popular operating systems, are usually mostly violated by mass malware, with the only intention of causing harm to a greater number of possible systems; The DMZ component, provides enterprise services, supported on platforms with corporate focus, targeted malware specifically developed to violate intrinsic characteristics of the network or victim system. The use of external tools to develop and obtain necessary data on the behavior of the infected system and the development of the executing specimen with services such as "Zabbix" and "Moloch" have influential limitations on the accuracy of the Dynamic analysis and the resulting formulation of conclusions and elaboration of "commitments indicators" or signatures that help the detection of malignant software.
Descripción:	151 hojas : Dimensiones 19 x 21 cm
URI:	

Introducción

Las organizaciones gubernamentales o empresariales, poseen muchos retos respecto a temas de seguridad, son el blanco predilecto de ciber-delicuentes en búsqueda de grandes ganancias económicas o afectaciones a la confiabilidad y participación en el mercado de grandes corporaciones por diversas motivaciones. Una de las principales amenazas surgen con las infecciones de malwares en redes corporativas, donde estos son código maliciosos diseñados para vulnerar sistemas y causar perjuicios significativos, sea con fines monetarios, activismo e incluso terrorismo. Estos softwares pueden obtenerse vía diversas fuentes (internet, usb, ingeniería social, vulnerabilidades de software, etc), y poseer uno o más de los siguientes componentes: Ocultador[1], replicador[2], bomba[3].

El análisis de malware implica el estudio sistemático y aplicación de diversas herramientas con el fin de identificar el comportamiento de software malicioso. Existen básicamente dos métodos de análisis: Estático, estudia todo lo que el software en sí conlleve, su empaquetado, librerías usadas, etc. Y análisis dinámico, cual implica la ejecución del código y monitoreo de su comportamiento en el sistema. Estas técnicas tienen como objetivos la obtención de firmas[4], usadas por antivirus para identificación.

El análisis dinámico debe de realizarse en un laboratorio con ambiente controlado, debido a las dificultades económicas y logísticas de un laboratorio real, la opción más usada es la simulación del entorno, usando para ello softwares de virtualización, permitiendo facilidades como: Obtención de snapshots[5], restablecimiento del sistema, menor riesgos a equipos reales, menor costo de investigación. La virtualización es una tecnología de gran importancia presente y futura, debido a todas sus prestaciones respecto a interoperabilidad de servicios y su aplicación como base de tecnologías en la nube.

El presente estudio expone las capacidades brindadas por tecnologías de virtualización para el desarrollo de análisis dinámico de malware desde una perspectiva de red en conjunto empleando una topología de red de común uso entre empresas de medianas o sucursales de grandes corporaciones.

[1] forma de permanecer indetectables

[2] manera de propagarse

[3] ejecución de ataque

[4] Forma abstracta de identificación de malware, partiendo de sus características

[5] Capturas del estado presente del sistema y almacenamiento para su posterior uso.

CAPÍTULO I

CONTEXTUALIZACIÓN DE LA INFORMACIÓN

1.1. Problematización.

1.1.1. Planteamiento del problema.

En una red corporativa es primordial garantizar la confidencialidad e integridad de los datos, así como una alta disponibilidad, debido a la naturaleza de los datos almacenados y su importancia crítica para el funcionamiento de la organización, la seguridad de la información toma un rol significativo dentro de la operatividad empresarial. Las organizaciones sean estas industriales, empresariales o gubernamentales y tanto sus infraestructuras de redes como sistemas en general, son un preciado objetivo para el mundo del crimen cibernético o activismo digital motivados por factores políticos, económicos o socio-culturales. El malware o software malicioso está diseñado para explotar vulnerabilidades existentes en redes o sistemas informáticos con fines pocos éticos en busca de afectaciones negativas, ninguna red o dispositivo electrónico está completamente absuelto en temas de infecciones de código maliciosos, sea en ambientes domésticos, corporativos o industriales existe situaciones de alto riesgo con impactos significativos y repercusiones catastróficas.

En temas de seguridad de estado a nivel mundial, es necesario el fuerte resguardo de infraestructuras críticas, común objetivo en el ciber-terrorismo, ciber-espionaje y ciber-sabotaje, para evitar situaciones como las presentadas en 2007 con la operación denominada "Octubre Rojo", espionaje masivo en casi cuarenta países de mayormente organismos gubernamentales y agencias diplomáticas realizado mediante un complejo «troyano»[6]. La incidencia de tecnologías de vanguardia con aplicaciones en código maligno, dificulta la detección eficaz de ataques, repercutiendo en aumento de cantidad y complejidad de software malicioso variando técnicas significativamente en plazos de tiempos cortos. En la octava cumbre Latinoamericana de analistas de seguridad desarrollada en 2018 y organizada por «Kaspersky Lab», presenta en el 2017 al código malicioso tipo «ransomware»[7] como el segundo lugar de incidentes en seguridad, mientras, en 2018 existe un considerable aumento en ataques «cryptojacking»[8] al brindar ingresos seguros y sostenidos, con posibilidades de aprovechar los recursos ilimitados que las nuevas tecnologías en la nube brindan a las empresas.

[6] Código malicioso camuflado dentro o cómo de software legítimo.
[7] Software maligno con capacidad de encriptar la información y pedir un rescate.
[8] Uso no autorizado de capacidades computacionales ajenas para la minería de criptomonedas.

Diagnóstico.

Los malware pueden estar dirigidos a objetivos generales o destinados a quebrantar una determinada organización o empresa, motivo de gran inquietud dentro del mundo empresarial. Por ello, ESET en su encuesta titulada *«Security Report Latinoamérica 2017»*, denota como principal preocupación la infección por software malicioso con un 56%, esto debido *al "grado de sofisticación que tiene el malware y el retorno económico que genera"* [1], para el 2018 el código malicioso tipo ransomware presentaba por sí solo gran inquietud para las empresas, ya clasificándose como una categoría independiente. La sofisticación de nuevos software maliciosos disminuye la efectividad de sistemas de seguridad, como antivirus, basados en el conocimiento del comportamiento y efectos del malware, necesitando de investigación y monitoreo de sistemas para su detección. Una vez aislado la muestra, es necesario el establecimiento de un ambiente protegido con mucha similitud a los sistemas existentes, siendo ideal el uso de infraestructura física real. Los elevados costos de implementación de un laboratorio físico de análisis exceden las posibilidades para empresas con recursos limitados o investigadores independientes.

Pronóstico.

El crecimiento de la cantidad de malware liberados indica la existencia de mayor número de desarrolladores, quienes estudian, modifican y aplican diversas técnicas para elaborar malwares con mayor complejidad y sofisticación. Las nuevas y prometedoras tecnologías son el objetivo de los atacantes cuando no se desarrollan tomando en cuenta los objetivos de la seguridad informática y de redes. El surgimiento de nuevos dispositivos inteligentes y su masificación los convierten en blancos perfectos, otros de los conceptos futuristas que están siendo aplicados en el presente son el «Internet de las Cosas»[9], el cual ha sido fuertemente vulnerado, debido a varios factores, destacando la limitada cantidad de procesamiento que poseen dichos dispositivos, aplicar técnicas de seguridad informática ralentizaría sus operaciones. Se estima que para el 2020 existan veinte billones de dispositivos IoT conectados a la red, resultando objetivos de códigos maliciosos con el fin de crear grandes botnets[10] y realizar ataques DDOS[11] en extremos difíciles de mitigar. Además con la propagación de ransomware, han surgido variantes aplicadas a los dispositivos mencionados, denominados "Ransomware de las Cosas (RoT)" e involucra el

[9] Internet de las Cosas.- sistema de dispositivos interrelacionados y conectados a internet
[10] Diversos equipos "zombies" en espera a código para realizar ataques en conjunto.
[11] Denegación de servicios distribuido

bloqueo de los dispositivos en búsqueda de un rescate monetario. Las bondades y posibilidades de estas redes son conocidas por el público en general, en donde según ESET Latan[12] "*El 81% de los usuarios opina que la llegada de internet de las cosas brinda más comodidad a la vida cotidiana*" [2] pero también es reflejada la desconfianza que estos productos poseen con respecto a la seguridad, donde *"El 70% de los participantes considera que los dispositivos IoT no son seguros"* [2].

Por lo avances en detección de virus y el uso de técnicas de inteligencia artificial en los antivirus, se prevé un aumento de complejidad en los malware, específicamente en su componente de ocultamiento, pruebas de ello ya están presentes en la actualidad, como: Virus polimórficos, cuales están en capacidades de variar su patrón de bytes con cada infección, dificultando en el correcto funcionamiento de los software antimalware para su detección. Virus metamórficos, aquellos que *"pueden transformarse en función de su capacidad de traducir, editar y reescribir su propio código*" [3]. Infecciones sin archivo, virus que actúan sin dejar rastro alguno generalmente abandonando el sistema justo después de haber realizado su tarea maliciosa, también poseen la capacidad de realizar un análisis previo del sistema, con lo cual si detecta alguna máquina virtual, procede a auto-eliminarse con el fin de dificultad su estudio.

1.1.2. Formulación del problema.

¿En qué medida las posibilidades brindadas por entornos virtuales permiten el análisis dinámico de malware reciente y el estudio del impacto a la red corporativa como conjunto?

1.1.3. Sistematización del problema.

¿De qué manera es posible la abstracción de una red empresarial en componentes fundamentales y cuáles son las características de las muestras de software malicioso con posibles afectaciones?

¿Cómo interconectar virtualmente los distintos componentes de una red para simular un entorno corporativo?

¿De qué manera puede estudiarse las capacidades del software de virtualización para el análisis dinámico de malware reciente en un entorno de red completo?

[12] Empresa desarrolladora de antivirus y soluciones de seguridad.

1.2. Objetivos.

1.2.1. Objetivo general.

Aplicar análisis dinámico a malware reciente en ambiente de red corporativo virtual mediante la abstracción en componentes elementales.

1.2.2. Objetivo específico.

- Identificar una topología de red de amplio uso en empresas medianas y sucursales, definir muestras de código malicioso a probar según características propias de los componentes abstraídos.
- Crear un ambiente de red funcional dentro de un entorno virtual mediante la interconexión lógica de sus distintos componentes.
- Analizar el comportamiento de software maligno desde una perspectiva de red en conjunto.

1.3. Justificación.

El reporte anual titulado *«ESET Security Report Latinoamérica 2018»* [4] manifiesta como una de cada cinco empresas Latinoamericanas estuvieron propensas a por lo menos un incidente de seguridad, aumentando respecto a años anteriores, siendo el software maligno líder con un 45%. Ecuador reporta un 22% de infecciones producidas por ransomware (ver ***Anexo 1***) convirtiéndose en cabeza de la lista, aunque, los índices varían mínimamente entre los distintos países de la región. El tamaño de la empresa traducido a mayores recursos cuanto a defensa digital se refiere, influye en cantidad de incidentes reportados (ver **Anexo 2**), las grandes organizaciones implementan tecnología de vanguardia y cuentan con personal calificado para la seguridad de la información, las empresas medianas, pequeñas o inclusive grandes poseen limitaciones que pueden ser mermadas por una correcta estrategia nacional de ciberseguridad adoptada por el país, con impacto positivo y no medible sobre la totalidad de los sectores de la economía.

La mayoría de las estrategias nacionales de ciberseguridad fomentan la implantación de equipos de respuestas ante incidentes de seguridad (CSIRT) públicos o privados, encargados del análisis de infraestructura crítica empresarial o estatal. Las empresas pequeñas, medianas e inclusive grandes, generalmente carecen de capital para poseer equipos de respuestas propios, siendo propensas a software maligno no detectado por soluciones de seguridad como antivirus, al trabajar usualmente con firmas digitales[13] cimentadas en el comportamiento. El instituto SANS[14] aclara que *"Las herramientas completamente automatizadas normalmente no proveen tanta información como lo podría hacer la intuición de un analista humano al examinar el espécimen en un modo mucho más manual"* [5].

La finalidad del proyecto de investigación es usar tecnologías de virtualización para la instauración de un laboratorio de análisis dinámico de malware, basado en topologías de redes empresariales comunes entre PYME[15] o sucursales de grandes corporaciones, empleando una mínima cantidad de recursos.

[13] Denotación estructurada del comportamiento de malware para facilitar su identificación.
[14] SysAdmin Audit, Networking and Security Institute.
[15] Pequeñas y medianas empresas.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA DE LA INVESTIGACIÓN

2.1. Marco Conceptual

2.1.1. Redes Corporativas.

La academia Cisco define red empresarial como: "*troncal de comunicaciones de una empresa para interconectar computadoras y dispositivos entre redes de departamentos y grupos de trabajo, facilitando la accesibilidad de datos*" [6]. Conlleva a la convergencia de redes para dar soporte a la operatividad de una empresa, la gestión eficiente de datos empresariales, la interoperabilidad de sistemas y dispositivos, y la seguridad de información.

La complejidad de su estructura depende del tamaño de la empresa a la cual da soporte. Si bien puede incluso definirse como una WAN[16], está conformada por una o más "Redes de Área Co0rporativas" (CAN), partes aisladas y protegidas de una intranet[17] empresarial con restricciones propias del departamento, generalmente poseen limitaciones para conexión a Internet así como también de otras CAN's pertenecientes a la misma corporación.

2.1.1.1. Características básicas de Arquitectura de Red.

Las redes una corporación debe de soportar distintos aplicaciones y permitir el desarrollo de diversas aplicaciones, asegurando el funcionamiento independiente del medio (cobre, fibra, Wireless…etc). Existen cuatro características básicas expuestas por la Cisco Networking Academy en [7], que deben ser consideradas al momento de diseñar una arquitectura de red.

- **Tolerancia a fallas:**

Limita las afectaciones de las fallas, buscando la menor cantidad de dispositivos afectados, posibilitando una recuperación rápida (plan de contingencia). Se basa en proporcionar redundancia en infraestructura y equipos, esto se logra mediante la implementación de una red conmutada por paquetes.

- **Escalabilidad:**

Posibilidad de Expansión para admitir nuevos usuarios, servicios y aplicaciones sin afectar el rendimiento y a usuarios de la red actual. Esto es logrado siguiendo un diseño de red con protocolos estandarizados y tomando en cuenta el crecimiento posterior de la organización.

[16] Red de Área Amplia
[17] Red perteneciente a una organización con restricciones de acceso sólo el área interna de una empresa

- **Calidad de Servicio (QoS):**

A raíz de las redes convergentes, la calidad de servicio es un requisito imprescindible para las redes actuales, posibilita la administración de congestión y el envío confiable de contenidos a todos los usuarios. Existen servicios que deben de conservar una latencia[18] baja como: video en vivo, QoS da prioridad a tráficos de este tipo.

- **Seguridad:**

La vulneración de las redes puede provocar pérdidas cuantiosas a la organización así como la disminución de confiabilidad en la percepción de sus clientes. Existen dos problemas a considerar: Seguridad de infraestructura, protección física de dispositivos de networking así como restricción al acceso del software administrativo residente; Seguridad de información, protegen el contenido de los paquetes enviados por la red así como de la información almacenada.

2.1.1.2. Topologías básicas.

Se llaman topologías de red a las diferentes estructuras de intercomunicación y organización en redes de transmisión de datos entre sistemas o dispositivos. Cuando componentes empleados en domótica, tales como actuadores, autómatas programables, robots y demás sensores se comunican entre sí, éstos, deben interconectarse con una estructura determinada de manera física. Cada topología de red lleva asociada una topología física, es decir, la manera en la que debe ser dispuesto el cable de interconexión entre los elementos de la red. La topología lógica es un conjunto de reglas normalmente asociado a una topología física, que define el modo en el que se gestiona la transmisión de los datos en la red. La utilización de una topología influye en el flujo de información (velocidad de transmisión, tiempos de llegada, etc.), en el control de la red, y en la forma en la que ésta se puede expandir y actualizar. [8]

- **Interconexión total y parcial.**

Proporciona múltiples enlaces físicos entre los nodos conformantes de la red, de tal manera que carece de varios canales de comunicación compartidos o múltiples caminos entre dos nodos. La interconexión es total cuando todos los nodos están dispuestos de forma directa,

[18] Suma de retardos temporales dentro de una red

existiendo obligatoriamente un enlace punto a punto para su comuncación, La interconexión parcial ocurre cuando no todos los nodos pueden conectarse mediante un enlace directo con otro nodo de la red. [8]

- **Interconexión en estrella.**

Cada nodo se conecta a un nodo principal (central o concentrador) encargado del de administrar acceso a la red (en caso de colisiones). Esta topología de nodo central como principal, se encarga de controlar toda la comunicación, pues cualquier anomalía en el mismo conduce a fallos de la red completa. Su implementación puede ser una decisión factible en el caso de que los nodos de la red no se encuentren muy distantes y el coste que supone la interconexión física de cada nodo al centro. [8]

- **Interconexión en bus.**

Todos los nodos se conectan a un único medio de transmisión utilizado transceptores, encargados del control de acceso. Los mensajes se envían por el bus y todos los nodos escuchan, aceptando los datos únicamente dirigidos a él (destinatarios únicos). Esta topología permite la adición y sustracción de nodos sin inferencia en la red restante, pero, un fallo en el medio de transmisión afecta gravemente la operatividad (roturas de cable). Puede cubrir distancias mayores, empleando repetidores y amplificadores. Poseen costes menores y sencillez de instalación. [8]

- **Interconexión en árbol.**

Esta topología puede interpretarse como el encadenamiento de diferentes estructuras en bus de diferente longitud y de características diferenciadas, constituyendo diferentes ramas de interconexión. Adquieren significancia los elementos que duplicadores y enlazadores entre diferentes líneas, ya que actúan como nodos principales, siendo una analogía a como lo hace el nodo principal de topología en estrella. [8]

- **Interconexión en anillo.**

Los nodos se conectan en serie formando un anillo. Es equivalente a unir los extremos de una red en bus. Los mensajes se transmiten hacía una dirección (actualmente es posible realizar envío en ambos sentidos), pasando por todos los nodos necesarios hasta llegar al destino. No existen nodo principal y control de la red, este queda implícito en cada nodo.

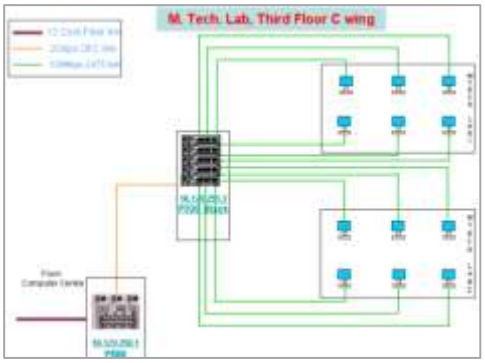
Durante la ampliación o reducción de la red, el funcionamiento se ve obstruido, un fallo en la línea provoca la caída de la red. También se la conoce como red "testigo" o "Token ring". Posee una relación coste-modularidad bastante positiva, en general, la instalación es compleja. No influyen los fallo en las estaciones si son condicionan la capacidad del interfaz del anillo. Es muy sensible a errores en los módulos de comunicaciones y en el medio de comunicación. [8]

2.1.1.3. Perspectivas de redes empresariales.

Sridhar Iyer en su charla sobre "Introducción a las Redes Empresariales", dimensiona los componentes de una red en varios niveles partiendo de lo más particular hasta llegar a la red en general. [9]

- Nivel "nano": Está conformado por una sola computadora en una organización
- Nivel "micro": Una subred (departamento) dentro de la organización, suelen contar con recursos compartidos descentralizados (impresoras, archivos, etc.).

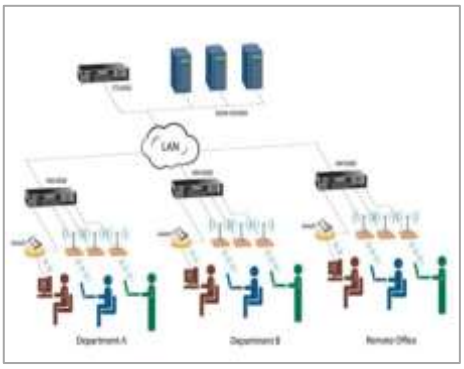
Ilustración 1: Representación de nivel "Micro"



Fuente: Sridhar Iyer
Elaborado por: Sridhar Iyer

- Nivel "mili": Una única entidad dentro de una gran organización, soporta aproximadamente 100 usuarios con almacenamiento de datos centralizado, seguridad, aplicaciones de administración de red. Posee routers y servidores. Típica para empresas medianas o pequeñas (PYME), no necesita de técnicos de soporte de planta, pudiendo otorgar esta responsabilidad a subcontratistas.

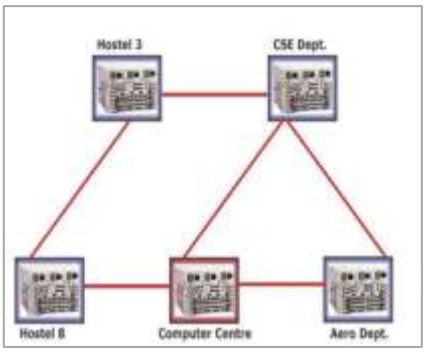
Ilustración 2: Representación de nivel "mili"



Fuente: Sridhar Iyer
Elaborado por: Sridhar Iyer

- Nivel "típico": Puede ser una sola organización con capacidad de mil usuarios, varias locaciones, cien switches y hasta diez routers.

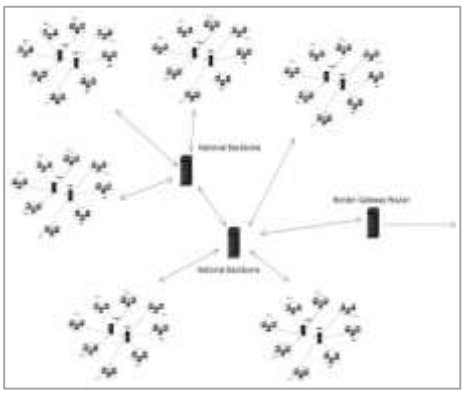
Ilustración 3: Representación de nivel "típico"



Fuente: Sridhar Iyer
Elaborado por: Sridhar Iyer

- Nivel "Kilo": Una red nacional perteneciente a una sola organización, necesita de líneas arrendadas o servicios de enrutamiento proporcionado por ISP's

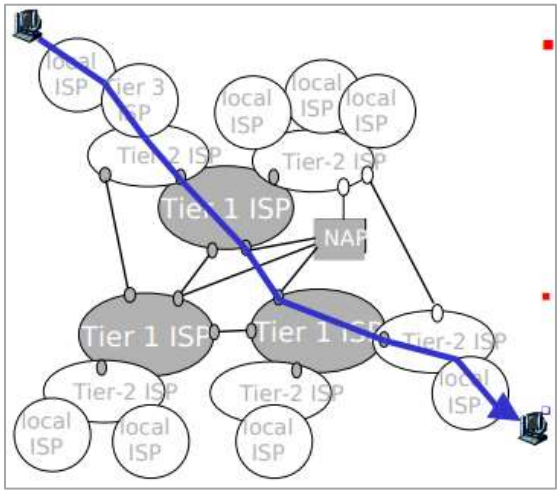
Ilustración 4: Representación de nivel "Kilo"



Fuente: Sridhar Iyer
Elaborado por: Sridhar Iyer

- Nivel “mega”: Una red internacional para una sola organización. Necesita de la coordinación de varios proveedores internacionales de banda ancha. Cubre aproximadamente diez países con más de mil locaciones.

Ilustración 5: Representación de nivel "mega"



Fuente: Sridhar Iyer
Elaborado por: Sridhar Iyer

- Nivel “Giga”: Representada por el impacto de nuevas tecnologías, “Internet de las Cosas”, soportadas a través de varias organizaciones y redes, alrededor de todo el mundo con miles de millones de dispositivos.

2.1.2. Entornos Virtuales.

“*En informática, virtualización se refiere a la abstracción de los recursos de una computadora, llamada Hypervisor o VMM (Virtual Machine Monitor) que crea una capa de abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (virtual machine, gues*t)” [10], siendo un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un sistema operativo, una red o incluso un dispositivo de almacenamiento, en el cual al recurso se lo divide en uno o más entornos de ejecución.

La virtualización crea un puente externo, permitiendo esconder la implementación subyacente ya sea mediante la combinación de recursos en localizaciones físicas diferentes, o a través de la simplificación del sistema de control. En los últimos años, el desarrollo de nuevas plataformas así como de nuevas tecnologías de virtualización ha hecho que el concepto de virtualización sea una práctica común en distintos entornos empresariales. [11]

En resumen, una máquina virtual es un sistema operativo completo que corre como si estuviera instalado en una plataforma de hardware real, independiente o física, por lo general operando varias máquinas en un mismo servidor de vitualización. [8]

2.1.2.1. Virtualización de Servidores.

La virtualización de servidores es el tipo de virtualización más usado en el ámbito empresarial, posee ventajas como: servidor en ahorro de energía, de espacio y en facilidad de administración de menos servidores físicos.

La virtualización de servidores es como su nombre lo indica, la emulación o simulación de un servidor, entendiéndose por servidor todo aquel sistema informático al que los clientes u otros computadores se conectan para obtener archivos, impresoras, invocar servicios o en general manejar recursos de la red.

2.1.2.2. Virtualización de sistemas operativos.

Este tipo de virtualización se produce al poseer previamente un sistema operativo (SO) anfitrión o base, en el cual se instala un programa de virtualización con posibilidades de instalar a su vez otros sistemas operativos (invitados), trabajando encima del sistema operativo principal, esto debido a la capa de virtualización puesta por un software como virtual PC o VMware Workstation, Proxmox, Hyper V. "Los desconocen que se encuentran virtualizados sobre otro sistema operativo o anfitrión" [12].

Las aplicaciones que trabajan dentro de los invitados lo hacen como si estuviesen funcionando en un computador dedicado para ellos. Esta técnica de virtualización también es conocida como virtualización en contenedores pues los sistemas operativos invitados están contenidos en una especie marco que les permite trabajar de forma casi independiente, todo basado en la disponibilidad y capacidad de los recursos del hardware del host anfitrión. Algunas de las compañías más importantes en este nicho de mercado de virtualización son por supuesto. [11]

2.1.2.3. Emulación de Hardware.

Está más relacionada con la virtualización de clientes. Es la instalación de software de virtualización (hipervisor) antes de la instalación de cualquier otro SO, este "hipervisor"

presenta el hardware del computador a todos los sistemas operativos instalados emulando los recursos que este tiene. [11]

El hipervisor también coordina el acceso a los recursos del computador que se da por parte de los sistemas operativos, tomando el papel de árbitro, decidiendo quién va primero y quién tiene que esperar para usar los recursos. Este esquema presenta muchas ventajas, ya que las máquinas virtuales instaladas pueden ser completamente movidas de un computador físico a otro, incluso sin tener que ser apagadas. También es necesario para ejecutar diferentes sistemas operativos en un solo PC físico: Linux, Windows, Solaris, etc. [11]

2.1.2.4. Para-virtualización.

En esta forma de virtualización de servidores, no se produce emulación de hardware, ya que la para-virtualización no es enteramente virtualización, pues los invitados interactúan de manera directa con los recursos físicos del computador como si fuesen computadores dedicados. Es una forma de compartir recursos por periodos cortos de tiempo a quien lo requiera, intercalando procesador, memoria o tarjeta de red.

2.1.2.5. Hipervisor.

Técnica de virtualización integrada en entornos que separan el sistema operativo de un computador y las aplicaciones del componente físico, por lo general es aplicada mediante software, de esta manera una única máquina física puede contener, ejecutar y operar varias máquinas virtuales con diferentes requerimientos y sistemas operativos.

2.1.2.6. Softwares de virtualización populares.

2.1.2.6.1. KVM.

(Kernel based Virtual Machine). Basada en GNU/Linux y desarrollada por la empresa Qumranet, Permite la virtualización sobre hardware X86 y viene incluido por defecto a partir del Kernel 2.6.20 de Linux. KVM realiza una virtualización completa, a diferencia de otros sistemas que emulan el procesador (Virtual Box, VMWare), dando mucha usabilidad y flexibilidad, pero no aprovecha bien los recursos del servidor, a continuación se exponen ciertas características según [13]:

- Es un módulo perteneciente al kernel, no es necesario la aplicación de parches.
- No requiere de modificación en el kernel del sistema operativo host dentro de la VM.
- Está escrito empleando pocas líneas de código.
- De instalación sencilla, al necesitar únicamente solo 3 paquetes (kvm, kvm-kmp y qemu)

Estos son algunas desventajas del empleo de esta tecnología:

- El procesador debe soportar para-virtualización por hardware, característicos en procesadores con tecnología AMD.
- Carecen de interfaz gráfica intuitiva, complicando su uso.
- Solo son ejecutadas en Linux.

Ilustración 6: Entorno de KVM

Fuente: Wikipedia.org
Elaborado por: Wikipedia.org

2.1.2.6.2. VirtualBox Oracle VM.

Es un software de virtualización para arquitecturas x86/amd64, creado originalmente por la empresa alemana «innotek GmbH». Actualmente es desarrollado por «Oracle Corporation» como parte de su familia de productos de virtualización. Esta aplicación posibilita la instalación de sistemas operativos «invitados», dentro de otro sistema operativo en ejecución «anfitrión», cada uno con independencia de ambiente.

Entre los sistemas operativos con soporte, se hallan: GNU/Linux, Mac OS X, Microsoft Windows, OpenSolaris, OS/2 Warp y dentro de ellos es posible virtualización de: OS/2 Warp, Windows, Solaris.

Ilustración 7: GUI de VirtualBox

Fuente: fpg.x10host.com
Elaborado por: fpg.x10host.com

2.1.2.6.3. VMWARE.

Plataforma líder de la virtualización. Esta plataforma de virtualización más avanzada y popular del sector, permitiendo desde virtualizar sistemas operativos localmente hasta de gestión mediante la red (plataforma en la nube). Por mucho tiempo esta plataforma ha sido de pago y solo se posibilitaba la versión gratuita "Player" para ejecución de máquinas virtuales (sin posibilidades de creación), en la actualidad VMware Player ofrece la mayoría de funciones y posibilidades para usuarios comunes (incluso para crear máquinas virtuales) de forma gratuita, reservándose las funciones avanzadas, y de pago, para el sector empresarial. [14]

VMware es un sistema de virtualización por software (programa que simula un sistema o ambiente físico real). Al ejecutar el simulador, proporciona un ambiente similar en apariencia a computadores físicos, con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc. [13]

Ilustración 8: Creación de nueva máquina virtual VMWare

Fuente: adictosaltrabajo.com
Elaborado por: adictosaltrabajo.com

2.1.2.6.4. Xen.

Xen es un monitor de máquina virtual open-source desarrollado por la Universidad de Cambridge. La meta del diseño es poder ejecutar instancias de sistemas operativos con todas sus características, de forma completamente funcional en un equipo sencillo. Proporciona mayor aislamiento, control de recursos, migración de máquinas virtuales en caliente y garantías de calidad de servicio. Los sistemas operativos pueden ser adaptados para desenvolverse de mejor forma en Xen (manteniendo la compatibilidad), permitiendo alcanzar virtualización de alto rendimiento con menor requerimiento de hardware. Intel ha realizado diversas contribuciones, añadiendo soporte para sus extensiones de arquitectura VT-X Vanderpool. [13]

Esta tecnología permite que sistemas operativos sin modificar actúen como hosts dentro de las máquinas virtuales de Xen, siempre y cuando el servidor físico soporte las extensiones VT de Intel o Pacifica de AMD. [13]

Ilustración 9: Logo de XEN Project

Fuente: commons.wikimedia.org
Elaborado por: commons.wikimedia.org

2.1.2.6.5. OPENVZ.

Es una tecnología de virtualización de Linux, a nivel de sistema operativo. Permite que un servidor físico ejecute diferentes y múltiples instancias de sistemas operativos, conocidos como «Servidores Privados Virtuales (SPV)». Si se lo compara según virtualizadores tales como VMware, VirtualBox y tecnologías de virtualización como Xen; OpenVZ ofrece menor libertad de elección del sistema operativo, tanto los invitados como los anfitriones deben ser Linux (aunque las distribuciones de GNU/Linux pueden ser diferentes). No obstante, la virtualización en el nivel de sistema operativo de OpenVZ proporciona mejor rendimiento, escalabilidad, densidad, administración de recursos dinámicos, y facilidad de administración que las alternativas. [13]

2.1.2.6.6. LXC.

Es una tecnología de virtualización a nivel de sistema operativo para Linux, de esta manera un servidor ejecuta múltiples instancias aisladas, usado para la creación de VPS (virtual private server), de esta manera se obtiene un entorno virtual más no una máquina virtual como tal.

2.1.2.6.7. Proxmox

Es una plataforma completamente open-source para todas las empresas e integra hipervisores KVM y contenedores LXC, almacenamiento definido por software y funcionalidad de red en una única plataforma, fácilmente administrable y propicia la creación de clusters y gran resiliencia ante desastres, cuenta con una interfaz web de administración amigable. Optimiza recursos e incrementa la eficiencia con un mínimo costo. [15]

2.1.2.6.8. Windows Virtual PC.

(Antes nombrado Microsoft Virtual PC) es un software gestor de virtualización desarrollado por Connectix y adquirido por Microsoft para creación de equipos virtuales. Su función es la de emular mediante virtualización, un hardware sobre el que funcione un determinado sistema operativo. Con esto se puede conseguir ejecutar varios sistemas operativos en la misma máquina a la vez y hacer que se comuniquen entre ellos. [16]

Ilustración 10: Entorno de Virtual PC

Fuente: pcmag.com
Elaborado por: pcmag.com

2.1.3. Clasificación de Malware.

Los malware pueden clasificarse de diversas maneras, tanto por su actuar como el alcance esperado por los desarrolladores, dentro de esta categoría están involucrada dos clasificaciones: malware masivo y malware dirigido.

2.1.3.1. Malware masivo.

Aquel malware desarrollado para involucrar la mayor cantidad de equipos posibles, por lo general con fines económicos de terrorismo, indistintos de las motivaciones, es la variación más popular existente siendo Windows 7 el sistema operativo más atacado por su masificación.

2.1.3.2. Malware dirigido.

Posee objetivos claros, y bien definidos, suelen estar dirigidos a organizaciones gubernamentales, industriales o empresariales con características propias de los sistemas, es la clasificación más difícil de detectar por ser en su gran mayoría malware nuevos hechos a medida sin firma alguna no detectada por antivirus.

2.1.3.3. Clasificación por comportamiento.

Debido a la cantidad de variaciones que el malware tuvo a través de los años, expertos han realizado clasificaciones según funcionamientos y afectación a los sistemas, aunque con el tiempo los ataques se han ido tecnificando llegando hasta ataques que utilizan ya no solo ingeniería aplicada sino también social: [17]

- Virus informático y su descripción
- Virus ejecutables
- Virus residentes en memoria
- Virus de sector de arranque
- Macro Virus
- Virus de Correo Electrónico
- Gusano
- Troyano
- Exploits
- Rootkits
- Backdoors

2.1.3.4. Virus informático.

Nombre de origen latino «veneno», guarda semejanza con virus biológicos siendo análogos por su forma de actuar: Ambos emplean huéspedes (Computadores o seres vivos) e inician sus actividades en forma discreta hasta antes de mostrar manifestaciones de síntomas; Los dos hacen necesitan del huésped para su desarrollo y reproducción; Ambos tienen como objetivo expandirse a otros sistemas y alterar el normal comportamiento del huésped; por lo consiguiente, se considera como «Virus Informático» a archivos, partes de código o software ejecutable capaz de reproducirse, auto-ejecutarse, propagarse y ocultarse. [17]

2.1.3.5. Virus Ejecutable.

Este tipo de virus son de los más comunes, atacan a programas ejecutables (.exe, .com, .dll, .sys, .pif) populares en PC y por esta razón logran mayores alcances. Funciona al unirse al programa del huésped mediante diversas técnicas, al ejecutarse el software deseado, se ejecuta a la par el malware, buscando otros ejecutables que puedan ser vulnerados. [17]

2.1.3.6. Virus Residentes en memoria.

Este tipo de virus al residir en la memoria pueden tomar el control de las acciones realizadas por el sistema operativo o el usuario, así cada vez que se accede a un tipo de archivo que el virus sea capaz de infectar, de acuerdo a su programación, procederá a infectarlo tomando en cuenta que el usuario debió haber recibido o ejecutado previamente un archivo infectado. [17]

2.1.3.7. Virus de Sector de Arranque.

Es de gran afectación para el sistema operativo, residiendo en los primeros 512 Bytes del disco duro donde se ubica el sector de arranque (boot). Estos virus aprovechan dicho espacio del disco para ejecutar código malicioso, asegurando la infección del sistema cada vez que se inicie el mismo. Para solucionar este tipo de problemas se requiere de personal cualificado. Otra acción que también pueden realizar es almacenar el sector de arranque original en otro sector del disco de forma tal que posterior a su ejecución pueden restaurar el sector de arranque para que el sistema se pueda volver a ejecutar. [17]

2.1.3.8. Macro-Virus.

Surgido por el requerimiento de aplicaciones de ofimática (Microsoft Office, OpenOffice, etc) al ejecutar macros, cuales incluyen código para realizar cierta función. Los virus también pueden explotar esta funcionalidad para incluirse y ejecutar su código mediante la misma. Su ejecución se inicia al abrir documentos infectados, apropiándose de la aplicación e infectando los macros de los documentos futuros. [17]

2.1.3.9. Virus de Correo Electrónico.

Por la masificación de acceso a este medio de comunicación, en los últimos tiempos se ha convertido en uno de las principales fuentes de infección y propagación de software no deseado. Pueden explotar diferentes técnicas de Ingeniería Social, manejando un esquema común de propagación: Un usuario recibe un correo infectado; Abre el correo y lanza la ejecución del malware, infectando el sistema; Poseen la capacidad de auto-enviarse siguiendo la cadena de reproducción. Los virus explotan de forma masiva este medio por su facilidad de llegar a cualquier parte del mundo en donde un PC posea una conexión a internet o correo electrónico. [17]

2.1.3.10. Gusanos.

Son desarrollados para reproducirse por algún medio de comunicación como el correo electrónico o las redes de comunicación entre pares. Su objetivo primordial es alcanzar a la mayor cantidad de usuarios posibles y distribuir código malicioso de diferente denominación, cuales poseen diversos fines, como, engaño, robo o estafa. Entre sus principales funcionalidades también está el de realizar ataques de Denegación de Servicio Distribuido (DDos) contra sitios webs específicos (Windows Update). [17]

2.1.3.11. Troyanos.

Su nombre se deriva en analogía al "caballo de Troya" perteneciente a la mitología griega. Es un programa incluido en otra aplicación legítima para el usuario, ejecutándose a la par con la aplicación que le brinda alojamiento, permitiendo acceso al sistema y evitando la autentificación de seguridad. No es categorizado como un virus ya que no cumple con todos los requerimientos del mismo, pero al emplear otras aplicaciones para su propagación en forma no consensuada es catalogado como amenaza. El principal objetivo de un troyano es pasar desapercibido al usuario después de instalarse, actualmente poseen la capacidad de abrir puertas traseras o descargar malware más nocivo. Otra práctica común es simular que realiza una función útil para el usuario y así tienen campo abierto para acciones dañinas. [17]

2.1.3.12. Exploits.

Nombre derivado de su funcionalidad y características de "explotar" vulnerabilidades existentes en el sistema. Aunque no es en sí un código malicioso, es utilizado generalmente como módulo de otro tipo de malware para obtener acceso al sistema y permitirle escalar privilegios para obtener funciones de usuarios adminstradores. [17]

2.1.3.13. Rootkits.

El término se emplea en los sitemas Unix, para categorizar al tipo de superusuario con capacidades ilimitadas en el sistema, pudiendo realizar cualquier tipo de acción sin restricción alguna.

Este tipo de malware por lo general trabaja de forma no visible al usuario permitiendo acceso o tomar control del sistema. Existen distintos programas o herramientas de acceso y control remoto para sistemas legítimos con gran empleo en la industria, pero, es necesario recordar

que estos programas deber ser utilizados con ética profesional y es muy importante mantener esto presente ya que el uso inadecuado es éticamente incorrecto y en muchos casos ilegal. [17]

2.1.3.14. Backdoors.

Código malicioso enfocado a abrir "puertas traseras" en sistemas, como por ejemplo puertos de la capa de transporte generalmente cerrados, permitiendo a los atacantes el dominio total del sistema, dejando vulnerable la información almacenada. El principal objetivo de los backdoors es infectar a la mayor cantidad de computadoras posibles para luego poder utilizarlas en redes conocidas como redes zombies (botnet). [17]

2.1.3.15. Botnets.

Se define como redes bots "robots" al conjunto de sistemas infectados por código malicioso y controlado por su creador en forma de red. En una primera instancia, los desarrolladores distribuyen el malware de forma masiva para infectar a mayor cantidad de usuarios. Cada sistema infectado abre puertas traseras en el sistema, necesario para dar control al dueño de la botnet. Una vez que los equipos ahora llamados "zombies" han sido reclutados, los creadores hacen uso de un centro control para llevar a cabo las tareas que deseen, utilizando de los recursos de todos los equipos que forman parte de la red. [17]

2.1.3.16. Keyloggers.

Es un programa que registra y graba todas las pulsaciones de teclas, mientras se ejecuta, su funcionamiento es transparente al usuario debido a que se necesita el pulsado de combinaciones prediseñadas de teclas el ingreso a su consola de configuración e incluso puede ocultarse de los menús donde se puede desinstalar o quitar los programas del sistema operativo. [17]

2.1.3.17. Ransomware.

La definición del inglés "ransom" se estipula como la exigencia de un pago por la liberación de algo o alguien (rescate). Al combinar con la palabra "software", se obtiene el nombre de malware potencialmente dañino con la capacidad de secuestrar sistemas para pedir rescates (usualmente moneterios).

Reciben este nombre cualquier software con objetivos dañinos que mediante distintas técnicas secuestran documentos o sistemas, imposibilitando al dueño el acceso a los mismos. Este tipo de software tiene la capacidad cifrar con clave documentos y después deja instrucciones al usuario de cómo recuperarlos pero posterior al pago de un "rescate" monetario. [17]

2.1.3.18. Spam.

El Spam es identificado como aquel correo electrónico masivo y no deseado, popular en cualquier sistema de mensajería web. Entre los principales objetivos está el de ofrecer por una parte productos y servicios que por lo general son de gran impacto a más de tener precios accesibles. Si bien, como forma de publicidad masiva posee un bajo rango de efectividad, al tener alcance de millones de usuarios, hacen que las ganancias sean cuantiosas para el producto ofertado. [17]

2.1.3.19. Phishing.

El Phishing es un mensaje de correo electrónico que aparente contener información verídica de fuentes confiables para obtener información personal o credenciales de cuentas bancarias. El cuerpo del mensaje informa que se han perdido o se van a actualizar datos personales del usuario e invita a los destinatarios a ingresar al enlace que se añade en el mensaje donde se pide completar formularios con información confidencial. [17]

2.1.3.20. Spyware.

El Spyware (Software espía) es un programa informático que recopila información sobre las actividades del sistema, persona u organización, generalmente en forma no consensuada. Este malware utilizado principalmente por empresas publicitarias de internet. Actualmente es uno de los tipos de malware de mayor difusión con elevada presencia en ambientes empresariales y de hogar. [17]

2.1.3.21. Adware.

El Adware (Advertised Software) es un software que despliega publicidad de distintos servicios o productos. Muestras la publicidad en ventanas emergentes, o a través de una barra en la pantalla, suelen emplearse para el transporte de publicidad desagradable o poco ética y causando grandes agravios al usuario legítimo. [17]

2.1.3.22. Ingeniería Social.

El factor humano es considerado como el eslabón más débil en la cadena de seguridad informática. La ingeniería social ataca la vulnerabilidad natural de los humanos para acceder a sistemas de computadora, basado en las relaciones interpersonales y el engaño. Por ello, incluso las organizaciones con las más fuertes contramedidas de seguridad técnica, como procesos de autentificación, firewalls, etc. Pueden fallar en proteger sus sistemas. [17]

2.1.4. Generalidades de Análisis de Malware.

Existen dos técnicas para análisis de malware cubiertas en este proyecto: Técnica de análisis estático o de código; Técnica de análisis dinámico o de comportamiento.

2.1.4.1. Análisis Estático.

En el análisis estático la muestra no es ejecutada, se realiza una "disección" a "código muerto", por tanto es más seguro y obtenemos información inmediata (sin espera de respuesta por parte del malware como sucede en el análisis dinámico), el único riesgo en este tipo de análisis es la ejecución involuntaria de la muestra. [18]

Para evitar el problema anterior se recomienda realizar el análisis del espécimen en un sistema distinto al se presume diseñado para vulnerar, por ejemplo, si tenemos un troyano para Windows, podemos analizarlo en un sistema basado en GNU/Linux como Debian o Ubuntu, igualmente existen distribuciones de GNU/Linux especializadas en temas de análisis de malware, un caso es la distro Remnux recomendada por SANS Institute [18]. Las fases que comprende el análisis estático son:

- Tomado de huellas" del archivo, identificación del ejecutable, es decir extracción de sus propiedades estáticas (File Fingerprinting,)
- Búsqueda de cadenas (Strings)
- Identificación de Empaquetadores (Packer Detection)

2.1.4.2. Análisis dinámico.

En el análisis dinámico la muestra es ejecutada, normalmente realizado en ambiente virtualizado y aislado estrictamente, dentro de un laboratorio construido por el analista. En algunos casos también se realiza la infección sobre máquinas físicas, dependiendo de la muestra, pues algunas contienen protección contra máquinas virtuales, es decir, si detectan que el ambiente es una máquina virtual, tienden a comportarse de distinta manera que lo harían en un sistema de un usuario normal. [18]

2.1.4.2.1. Análisis dinámico Básico.

El análisis dinámico básico implica la ejecución del código sospechoso y la observación de su comportamiento en el sistema con el fin de producir firmar que faciliten su identificación y ayudar a la eliminación del mismo. Sin embargo, es necesario contar ocn un ambiente fuertemente aislado y seguro para evitar propagaciones involuntarias o afectaciones a otros sistemas reales. Al igual que el análisis estático, este tipo de análisis puede ser utilizado por la mayoría de las personas incluso sin grandes conocimientos de programación, pero no será efectivo con todo el malware. [18]

2.1.4.2.2. Análisis dinámico Avanzado.

El análisis dinámico avanzado consiste en la utilización de un depurador para la examinación del estado interno de un archivo ejecutable corriendo. Este tipo de análisis proporciona otra manera de obtener información detallada de un archivo ejecutable, es más efectivo en malware sofisticado. [18]

2.1.4.2.3. Análisis automático.

Aquel análisis de malware realizado con herramientas automatizadas, por lo general online, estas utilidades son conocidas como sandbox, cuales orquestan la ejecución de malware y estructuran las firmas correspondientes de acuerdo tanto a análisis dinámico o estático.

2.2. Marco Referencial.

2.2.1. Aplicación de metodología de malware para el análisis de la amenaza avanzada persistente (APT) "Octubre Rojo".

Abad [19] describe el proceso metodología expuesto por su mentor Don Javier Bermejo, para la evaluación de una especificidad de malware "Poison Ivy", estudiando en el proceso distintos tipos y comportamientos de software malicioso, tanto de alcance masivo como dirigido, exponiendo la usabilidad de herramientas libres y gratuitas para el desarrollo de RAT[19] y la implementación de laboratorio virtual correctamente aislado, como parte de la metodología aplicada. Tras evaluar diferentes metodologías, opta por un diseño de cuatro fases sistematizadas para análisis de malware, esto según [20] y teniendo en cuenta la adaptación a nuevos y distintas formas de malware, estas fases son:

- **Acciones iniciales.**

"Realización de una serie de acciones encaminadas a obtener un registro de la configuración de las máquinas que intervienen en el análisis" [20], esto para crear referencias o crear líneas bases con el fin de realizar comparaciones entre estados pre y pos-infección.

- **Clasificación.**

"Consiste en examinar el archivo ejecutable del malware, pero sin acceder a su código, con el objetivo de, primero identificar el topo al que pertenece, y, seguidamente, obtener información sobre su funcionalidad" [20], permite la obtención rápida de datos y una perspectiva sobre el código, posibilitando la realización de firmas simples de red.

- **Análisis de código.**

"*La realización de un análisis estático y otro dinámico del código ensamblador del malware, navegando a través de él, al objeto de conseguir un mejor entendimiento de su funcionamiento"* [20], implica un proceso complejo de ingeniería inversa y meticulosidad departe del investigador para descubrir funcionalidades ocultas de las etapas previas.

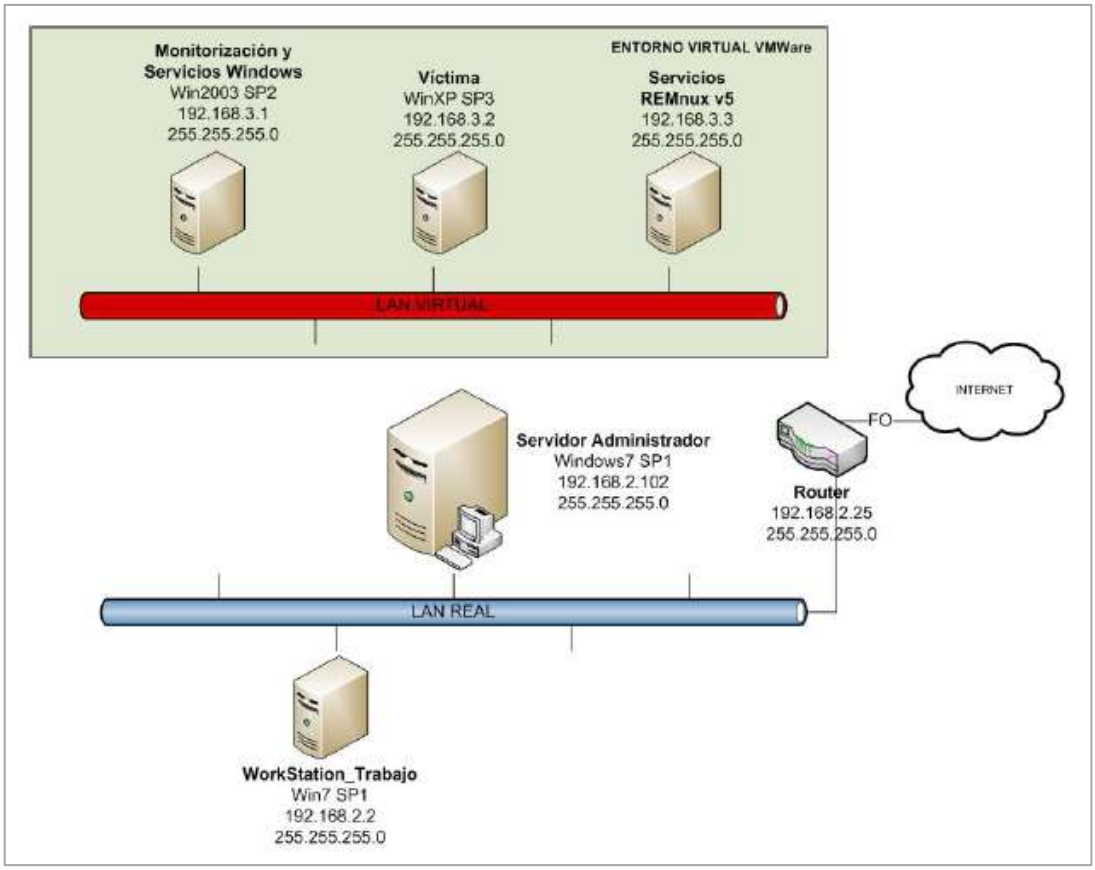
[19] Herramienta de acceso remoto

- **Análisis dinámico o de comportamiento.**

"Consiste en la realización de un análisis dinámico de la actuación del malware en el entorno de ejecución, con el objeto de observar su comportamiento" [20], en esta etapa se define el comportamiento, peligrosidad y objetivo de la muestra y sus acciones sobre el sistema objetivo.

La importancia de un laboratorio aislado de análisis de malware se encuentra verificada en el diseño escogido por Abad [21], basado en la herramienta de virtualización VMWare, genera un entorno interconectado con dos máquinas Windows (víctima y monitorización) y un equipo Linux (con REMmux[20]). Para simular un entorno real emplea un servidor virtualizado que brinde servicios DNS, FTP y Web, de esta manera propiciar un ambiente en que el malware pueda comportarse en libertad, topología presentada en ***Ilustración 11***.

Ilustración 11: Laboratorio propuesto por Gaviria para piloto experimental.



Fuente: Carlos Abad
Elaborado por: Carlos Abad

[20] Entorno integrado para realización de análisis de malware e ingeniería inversa

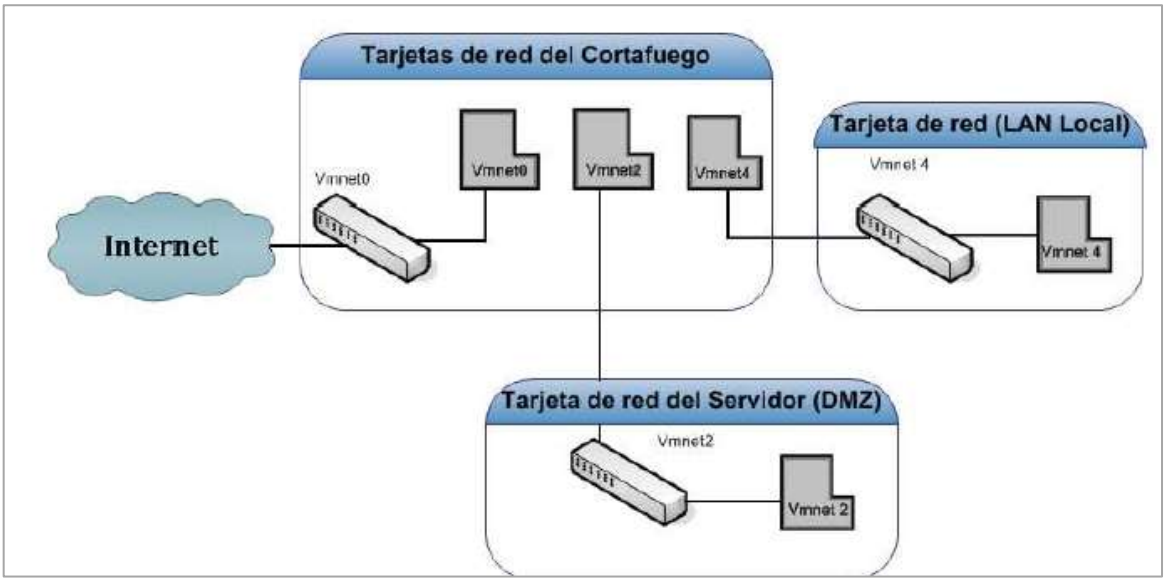
2.2.2. Vulnerabilidades y seguridad en redes TCP/IP.

Mancheno y Robles en [22], levantan un entorno corporativo virtual para la comprobación y estudio de la seguridad de una topología empresarial típica, empleando «zona desmilitarizada», «firewall» y «red interna». Usan las capacidades de interconexión entre componentes brindadas por el software virtualización «VMWare» y evalúa diferentes políticas de seguridad, estudia y específica los distintos tipos de posibles ataques y la realización de un test de penetración.

Emplea una topología sencilla, exponiendo que para el objetivo es la puesta en marcha de un sistema de seguridad, por lo cual con pocos componentes se obtiene una red funcional y usable para el fin de la investigación. Posee una red LAN local y una zona desmilitarizada, estas son las máquinas con mayor exposición al mundo exterior, por ende, las más atacadas.

En ***Ilustración 12*** se presenta la interconexión virtual de los componentes definidos y virtualizados en VMWare, usando switch virtuales (Vmnet), de esta forma puede crear redes aislada entre elementos ubicados en el mismo host físico.

Ilustración 12: Configuración de tarjetas de red de las máquinas virtuales



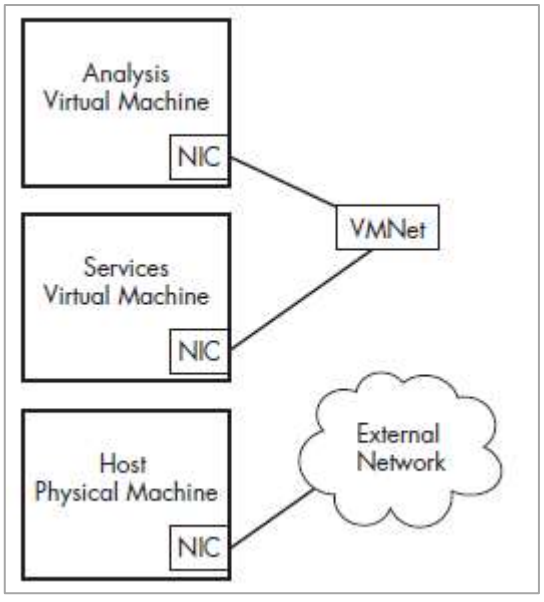
Fuente: Mancheno y Robles
Elaborado por: Mancheno y Robles

2.2.3. Practical Malware Analysis.

Sikorski y Honing en [23], presentan un manual didáctico con ejemplos y recursos necesarios para la introducción al amplio mundo de análisis de malware, partiendo desde la definición de conceptos bases, hasta procesos avanzados en análisis de software sospechoso. Posee ejercicios y retos propuestos con muestras prevista por la fuente, para la aplicación real de análisis. Es un libro referente en el contexto de aplicación de análisis de malware estático y dinámico.

Independiente de la plataforma utilizada, existe buenas practicas respecto a la interconexión del sistema y toma de snapshots, que facilitan en gran medida el correcto análisis. Unas de las topologías usadas, es el empleo de múltiple máquinas virtuales (***Ilustración 13***), conectadas entre ellas (los equipos a estudiar) pero desconectada del equipo anfitrión, de esta manera el malware no está conectado a algo importante pudiendo obtener servicios dentro de una LAN aislada.

Ilustración 13: Red personalizada en VMWare



Fuente: Sikorski y Honing
Elaborado por: Sikorski y Honing

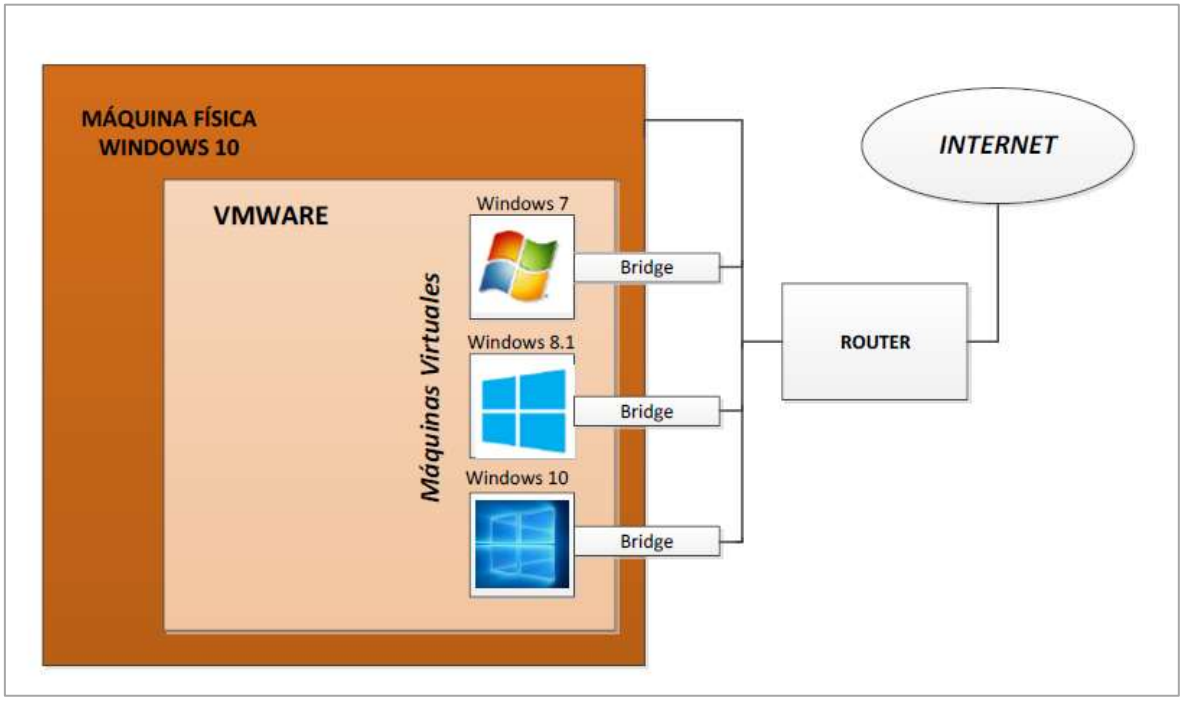
Al evaluar la posibilidad de realizar análisis de malware con salida a internet real, es debido la toma de precauciones, unos de los riesgos consiste en la posibilidad de esparcir código malicioso a otras plataformas, también existe la posibilidad de alertar al escritor del malware, advirtiendo de un posible análisis.

2.2.4. Análisis digital de una infección de malware en sistemas Windows.

Arce [24] describe el análisis de situación contemporánea a su año sobre el estado de malware y estadísticas de distintas organizaciones, poniendo en perspectivas la significancia del estudio de software malicioso. Realiza un análisis del comportamiento de malware con características de «ransomware» sobre tres equipos virtualizados, empleando distintas versiones del sistema operativo propietario de Microsoft (Windows 7, 8.1 y 10) denotando la importancia una correcta toma de línea base o «snapshot». Aplica el análisis siguiendo siete fases de una forma sistemática, cuales son: Selección de la muestra, implementación de un entorno de análisis, obtención de una línea de referencia del sistema limpio, obtención de una línea de referencia del sistema infectado, análisis de comportamiento y análisis de resultados, determinación de patrones comunes de comportamiento de malware.

Como herramienta de virtualización maneja "VMWare Workstation" en el cual ejecuta sistemas operativos dentro de una plataforma de virtualización compartida con Windows 10, ***Ilustración 14*** muestra la topología virtualizada empleando tres máquinas virtuales en una máquina física. Para obtener datos reales usó el adaptador puente (bridge) obteniendo una conexión directa con el router.

Ilustración 14: Diagrama de entorno de análisis de malware con tres máquinas Windows

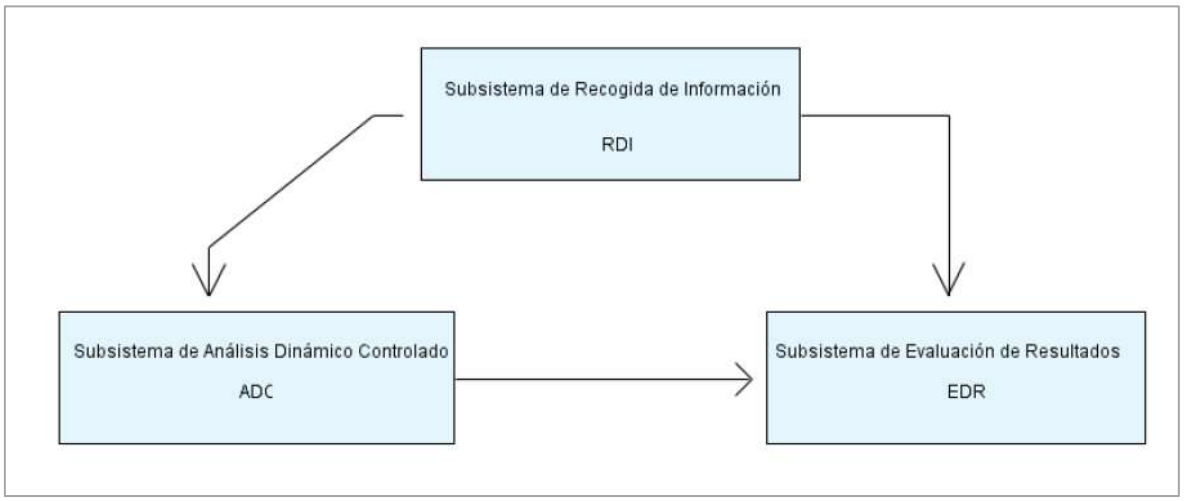


Fuente: Diego Arce
Elaborado por: Diego Arce

2.2.5. Análisis dinámico de malware en entornos controlados.

Ortega [25] emplea herramientas de análisis automático de malware para diseñar un ambiente vulnerable que propicie todas las características necesarias para el correcto desenvolviendo y el estudio optimo del comportamiento de malware ayudando a generar firmas estandarizadas «Yara», indispensable en la identificación. El diseñó de la herramienta de análisis automático de malware para Android consta de varios subsistemas, relacionados según lo mostrado en ***Ilustración 15***.

Ilustración 15: Arquitectura para sistema de análsis automático para android.



Fuente: Diego Sergio Ortega
Elaborado por: Sergio Ortega

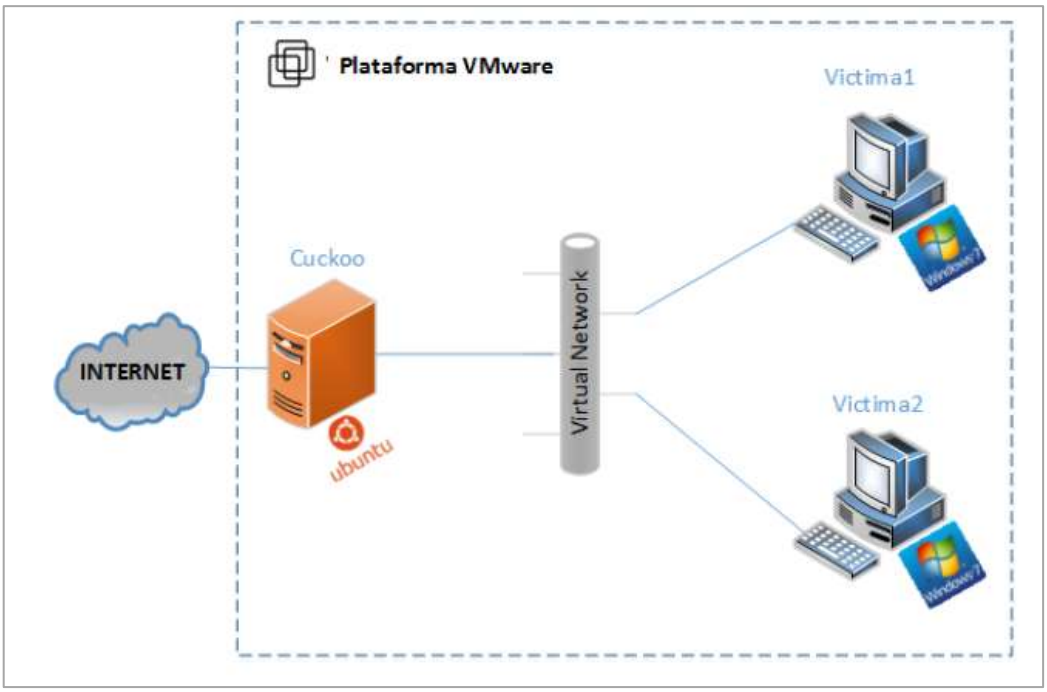
2.2.6. Análisis estático y dinámico de una muestra de malware en sistemas Microsoft Windows XP para determinar qué efectos produce sobre un sistema infectado.

Latorre [18] desarrolla análisis estático y dinámico en un laboratorio controlado, basado en el sistema operativo Windows XP, el comportamiento y afectaciones de malware con características de «troyano» y «ransomware», recreando infección de software malicioso «Virus de la Policía» con graves consecuencias nacionales. Realiza un estudio profundo de la historia y evolución de los código maligno en el Ecuador. Si bien el éxito del proyecto está centrado en la realización de análisis estático, utiliza varias herramientas definidas como "análisis dinámico automático", cuales brindan servicios online al establecer un entorno virtual y controlado de análisis "sandbox", se hace uso de: Payload Security, Como Malware Instant Analysis, MalwareViz, Malwr Y Anubis.

2.2.7. Metodología para el análisis de malware en un ambiente controlado.

Jumbo en [26], se enfoca en el estudio de métodos disponibles para el correcto análisis de malware, proveyendo recomendaciones para el establecimiento de un laboratorio de análisis y empleando la herramienta «CUCKOO» sandbox en sistemas virtuales para agilización del proceso, generando políticas de prevención, reacción y mitigación. Aplica y configura un escenario virtual con "Cuckoo Sandbox" corriendo en un equipo central (Ubuntu), encargado de orquestar el análisis dinámico y dos máquinas victimas con sistema operativo Windows 7, todo ello virtualizado bajo la plataforma VMWare Workstation (***Ilustración 16***).

Ilustración 16: Escenario virtual Cuckoo Sandbox



Fuente: Diego Sergio Ortega
Elaborado por: Sergio Ortega

2.2.8. Análisis actual de estado de malware.

Los desarrolladores de malware usan diversos medios de propagación tanto mediante la explotación de diversas vulnerabilidades en software y hardware existentes así como el engaño a usuarios incautos. En la ***Tabla 1***, se presenta una clasificación realizada por Kaspersky™ [21] en [27] sobre canales más comunes de infección.

[21] Organización creadora antivirus y herramientas de análisis de seguridad.

Tabla 1: Canales comunes de infección

Orígenes	Descripción
Internet	Canal principal de distribución de todo tipo de malware. Las estrategias más usadas son: • Acceso a sitios web maliciosos, p. ej. Ataques Drive-by[22]. • Descargar de malwares disfrazado, p. ej. Cracks[23]. • Descargas por medio de redes peer-to-peer (torrentes).
Correo electrónico	El software malicioso puede incluirse en el cuerpo del mensaje así como en los archivos adjuntos para realizar otro tipo de ataques, así como ser un efecto de spam[24] o un intento de fraude.
Vulnerabilidades de software	También llamados "exploits", pueden usarse para infligir sistemas e instalar software malicioso.
Medios Extraíbles de almacenamiento de datos	Archivos infectados dentro del medio externo pueden realizar una infección de virus, la cual se propagará a los demás discos disponibles dentro del equipo.
Usuarios	Uso de "Ingeniería social"[25] para instalación de aplicaciones corruptas.

Fuente: La Investigación
Elaborado por: Autor

Independiente del medio o forma de contagio, el malware puede tomar diversas acciones de acuerdo al objetivo de su(s) creador(es), si bien es difícil realizar una clasificación general de los mismos, en la

***Tabla* 2** presenta una clasificación de los tipos de malware más comunes y sus características, definido por Cisco Networking Academy en [28].

[22] Descarga tanto involuntario o voluntaria (engaño) de software no deseado.
[23] Programas ilegales para obtener de forma gratuita acceso a programas de pago
[24] Correo basura no deseados, con remitente anónimo.
[25] Manipulación de usuarios legítimos para conseguir información confidencial.

Tabla 2: Tipos de Malware

Tipo da Malware	Descripción
Spyware	Rastrea y espía al usuario con el fin de superar medidas de seguridad.
Adware	Provee anuncios automáticamente
Bot	Realiza acciones automáticamente, se suelen usar en grupos para crear Botnets (muchas computadoras infectadas) y realizar ataques de DDOS[26]
Ransomware	Secuestra o encripta los datos o todo un sistema hasta que se realiza un pago.
Scareware	Persuade al usuario con ventanas emergente de alarmas indicando algún problema y permitir así la infección.
Rootkit	Modifica el sistema operativo y crea puerta traseras para ser explotadas por atacantes.
Virus	Código malicioso ejecutable adjuntado a otros archivos ejecutables, la mayoría requiere de la intervención del usuario final.
Troyano	Ejecuta actividades maliciosas bajo la apariencia de una operación legítima y deseada, se adjunta a archivos no ejecutables.
Gusanos	Se replican mediante la explotación de las vulnerabilidades en redes, ralentizándolas. Pueden ejecutarse por sí mismos y son responsables de algunos de los ataques más devastadores de internet.
Hombre en el medio (MitM)	Permite tomar el control de un dispositivo sin el conocimiento del usuario.
Hombre en el móvil (MitMo)	Toma el control de un dispositivo móvil, para infiltrar información confidencial y enviarla a los atacantes.

Fuente: La Investigación
Elaborado por: Autor

[26] Ataque de Denegación de Servicio Distribuido, usa miles de computadoras "zombies" para bloquear un sistema

Cada uno de los softwares maliciosos expuestos poseen una o más de los siguientes tres componentes definidos según el consultor de ciberseguridad[27] Munir Njenga como:

- Ocultador: Esta característica o función habilita al malware permanecer indetectable incluso por los programas antimalwares[28].
- Replicador: Se ocupa de la diseminación y propagación del malware dependiendo de su naturaleza.
- Bomba: Es el ataque propiamente llevado, la afectación y daño al objetivo.

Como primer punto de la estrategia en contra a las infecciones de malware de todo tipo, se emplea el análisis de malware, el cual es definido como *"El arte de diseccionar malware para comprender su funcionamiento, identificarlo y como derrotarlo o eliminarlo"* [23]. El análisis de malware no establece la metodología para detectar un software malicioso o saber si un sistema está involucrado; describe las pautas para conocer al fondo un código malicioso, que es lo que puede realizar, la forma en que afecta a nuestra red y como medir o contener su daño. Sikorshi y Honing en [23] definen dos fines primordiales que el análisis de malware desarrolla:

- Firmas basadas en host.- Enfocado en detectar software dañino en computadores, identificar los archivos creados o modificados o los daños realizados al registro, en otras palabras, está centrado en el efecto del malware sobre el sistema.
- Firmas basadas en red.- Monitorea el tráfico y comportamiento de la red, si bien esto se puede realizar sin análisis de malware; empleando estas herramientas se posee mayor efectividad, detección y menor cantidad de falsos positivos

Existen dos métodos ampliamente usados en el estudio de código malicioso: Análisis de malware estático y, análisis de malware dinámico. El primer método realiza un estudio integral del código del malware, sin ejecutarlo, convirtiéndolo en una técnica segura para quien el investigador. Mientras, el análisis dinámico ejecuta el malware y estudia su efecto real sobre el sistema, se suele desarrollar en entornos virtuales para evitar un daño verdadero a un equipo real. Se emplea la categorización y definiciones realizada por [29] con el fin de aclarar conceptos.

[27] Protección de información, estudio y respuesta de amenazas que involucren redes y sistemas.
[28] Software de monitorización de sistemas que prevé infecciones.

- Análisis estático básico.- Estudia el código del malware empleando un escaneo con antivirus, realizando hashing[29] o detección del empaquetado, así como analizando la estructura del ejecutable propiedad del malware.
- Análisis estático avanzado.- Emplea herramientas adicionales, analizando Strings[30] y librerías vinculadas usando desensambladores[31].
- Análisis dinámico básico.- Involucra la construcción de entornos virtuales de ambiente controlado para el desarrollo del análisis, supervisando las acciones tomadas por el malware.
- Análisis dinámico Avanzado.- Realiza acciones adicionales depurando[32] el malware, analizando registros y haciendo un análisis íntegro de todo el sistema de estudio.

Los entornos virtuales empleando tecnología VMWare[33] gozan de gran popularidad entre analistas de seguridad, debido a las prestaciones y facilidades que conlleva su uso. No obstante, muchos creadores de software maliciosos conocen el proceso y las herramientas de análisis más populares, con el afán de ganar tiempo, pueden desarrollar códigos que se oculte, mute o auto elimine si detecta un ambiente simulado, indicativo de que está siendo analizado. Esto nos lleva a plantear una importante interrogante *"¿Qué tipo de laboratorio necesita un investigador de seguridad para realizar análisis de malware en el presente y futuro?"* [30].

De la misma manera en que los avances en programación y capacidades computacionales permiten el desarrollo de softwares maliciosos muchos más sofisticados, las herramientas para su análisis y detección también se encuentran a la vanguardia, contando con entornos virtuales con mayores capacidades para el análisis de malware. Se emplea máquinas virtuales las cuales están definidas por VMWare como *"Software que al igual que una computadora física, permite correr un sistema operativo y aplicaciones"* [31]. Las capacidades dependen tanto de la máquina virtual usada, así como, del sistema real en que se alberga. Actualmente, es posible simular varios sistemas independientes e interconectarlos para virtualizar un entorno de red completo.

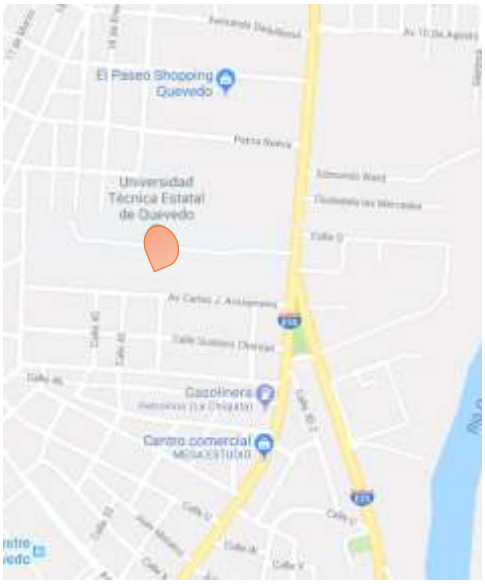
[29] Transformación del código en una cadena de caracteres de longitud fija.
[30] Secuencia de caracteres imprimibles
[31] Traduce lenguaje de máquina a lenguaje ensamblador
[32] Ejecutar el programa siguiendo todas sus acciones
[33] Líder en infraestructura de nube y tecnologías de virtualización

CAPÍTULO III
METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Localización.

La ubicación corresponde a la máquina real en donde se aloje al software de simulación, dependiente del hardware del equipo usado, mas no estrictamente ligado a un entorno físico. No obstante, es importante la ubicación física de este dispositivo, cual debe brindar facilidades para el desarrollo del análisis, como: libre de distracciones, acceso restringido, etc. El simular todo un ambiente de red completo implica la virtualización de varios componentes simultáneamente, conllevando gran capacidad de procesamiento y recursos, por lo cual debe de tomarse en cuenta las capacidades del equipo anfitrión. La investigación fue realizada principalmente en las instalaciones de la Universidad técnica Estatal de Quevedo, campus Manuel Haz Álvarez.

Ilustración 17: Localización de proyecto de investigación.



Fuente: La investigación
Elaborado por: Autor

3.2. Tipo de Investigación.

3.2.1. Investigación diagnóstica.

Instituye el primer paso de la investigación, empleada para establecer definiciones usadas a lo largo del proyecto, como: definición de red corporativa, topologías comunes, formas de abstracción en componentes elementales, etc. Permite establecer el estado actual de redes empresariales medianas, pequeñas o sucursales de grandes corporaciones, indagando las falencias presentadas a la seguridad y los peligros expuestos por limitaciones económicas en temas de seguridad de la información y continuación del negocio.

3.2.2. Investigación documental.

Mediante el estudio de investigaciones previas con temas con similitudes respecto a seguridad informática y estudio de malware, artículos científicos, publicaciones de revistas, reportes de organizaciones de seguridad (Kaspersky Lab, ESET, SANS, etc), foros y blogs de investigadores independientes. La investigación documental es la base para obtener conocimiento técnico resaltando el manual "Practical malware analysis".

En esta investigación se establece las características de malware según el componente objetivo dentro de una red corporativa y cuáles son las posibles consecuencias de su ejecución.

3.2.3. Investigación exploratorio.

Las bases de datos de malware poseen limitaciones, es bien conocida la gran cantidad de nuevo malware por segundo existentes, pero la mayoría de ellos se encuentran reservados, algunas organizaciones por temas de confidencialidad, utilizan servicios de análisis automático no distribuido, por lo cual las muestras no se quedan almacenadas y se prohíbe su distribución.

Las bases de datos con software malicioso reciente se encuentran protegidas y guardan discreción, por lo cual es necesario apegarse a un protocolo para obtener acceso a ellas, en la gran mayoría de ellas es necesario el envío del tema de investigación y sus objetivos, también ser respaldado por una organización o universidad.

3.2.4. Investigación experimental.

Este tipo de investigación se aplica al momento de crear un entorno virtual de una red definida en investigaciones previas, la instalación de los diversos sistemas e interconexión de los componentes de una forma segura hasta obtener una red completamente operativa y la toma de las líneas bases del sistema.

Una vez la red establecida, se experimenta con la ejecución del malware, monitoreando el sistema y notando los cambios producidos por los mismos, esto es realizado mediante una componente definida para ello.

3.3. Métodos de investigación.

3.3.1. Método inductivo.

Propicia el establecimiento de preguntas guías para la investigación, tales como: ¿Cuáles son las topologías comunes en empresas medianas, pequeñas y sucursales de grandes corporaciones? ¿Cuáles son el malware con afectaciones a los componentes definidos? ¿Cuál es la mejor forma de realizar una correcta investigación de la red? ¿Cuál tecnología de virtualización utilizar según los elementos? ¿Cómo aislar correctamente la red?

Al responder estas preguntas, se obtuvieron directrices de suma importancia para el desarrollo de la investigación.

3.3.2. Método analítico-sintético.

Usado en la documentación y obtención de registros tanto de un estado previo del sistema como la posterior ejecución de muestras, realizar comparaciones y obtener conclusiones. La monitorización debe de ser realizada en un ambiente correctamente aislado para evitar percances.

Seguidamente se evalúa el rendimiento del sistema operativo de virtualización, para medir su rendimiento.

3.4. Fuentes de recopilación de información.

3.4.1. Fuentes primarias.

Ejecución de diversos malware originados en distintos componentes de la topología y su impacto, tanto al equipo infectado, como en la red en conjunto.

3.4.2. Fuentes Secundarias.

Los tópicos generales se extraen de información difundida en la red, siempre y cuando la misma posea coherencia y relevancia. Para el estudio de los elementos específico se empleará; lecturas de artículos científicos, tesis doctorales y de grado, libros, conferencias o videos ilustrativos sobre aplicación de análisis dinámico en diversas redes, aunque haciendo énfasis en ambientes corporativos.

3.5. Diseño de la Investigación.

Para cumplir los objetivos propuestos se ha dividido la investigación en varias etapas, expuestas en orden cronológico con su respectiva descripción.

- **Etapa uno: Identificación de topología corporativa.**

En esta etapa se define una topología de amplio uso entre empresas medianas o sucursales de grandes corporaciones, sus componentes básicos y los sistemas operativos necesarios para realizar una red completamente funcional, también se procede a la abstracción en elementos esenciales que no afecten a la operatividad.

- **Etapa dos: Virtualización de topología.**

Se establece los requisitos necesarios para la virtualización de los diferentes elementos abstraídos de la etapa anterior, la elección de tecnología de virtualización según las características y objetivos del componente. Para la interconexión y aislación de diferentes subredes se emplea adaptadores de red "bridge" cual crea switch virtuales, de esta manera es posible el control de las redes y la delimitación del alcance de propagación. También se realiza la instalación de los sistemas operativos correspondientes y los servicios que brinde la DMZ.

- **Etapa tres: Identificación de muestras.**

Mediante el estudio de las características y los principales objetivos de malware propuestos se define el tipo de malware según se alcance para los componentes de red interna (malware masivo) y componente zona desmilitarizada (malware dirigido), también es necesario la identificación de bases de datos como fuentes de adquisición de muestras, usando Hybrid-Analysis por las facilidades de obtención y gran cantidad de malware subido diariamente, también proporciona los resultados de análisis automático previamente realizados y los indicadores de comportamiento.

- **Etapa cuatro: Análisis dinámico de malware.**

La etapa presenta el procedimiento aplicado para la realización de un análisis dinámico externo empleando como principal herramienta de obtención de información la componente monitoreo, se aplica la obtención de las líneas bases previa infección, análisis dinámico de malware empleando herramientas online (hybrid-analysis, VirusTotal y Spyral Scanner), y el análisis dinámico en el entorno virtualizado.

3.6. Instrumentos de Investigación.

Se especifica las herramientas usadas durante la etapa experimental de una manera general.

- **Análisis de documentos.**

La información referencial disponible se obtendrá en su mayoría mediante internet, debido a que en caso de tesis doctorales o grado, las universidades patrocinadores poseen repositorios digitales de libre acceso. Los artículos científicos fueron extraídos de varias revistas de tópicos apegados a lo estudiado, como; fundamentos de análisis de malware, estadísticas, comparaciones, e historia de software maliciosos, estudios de casos con graves afectaciones, etc.

- **Observación directa.**

Realizando el análisis del comportamiento y mediciones de diversos parámetros en un ambiente inicial sin infección alguna.

- **Procedimientos experimentales.**

Ejecución de código malicioso en un ambiente de red virtualizado y el empleo de herramientas de análisis, tales; Moloch, Zabbix, INetSIM.

3.7. Tratamientos de los Datos

Las diferentes operaciones realizadas sobre los datos extraídos de la experimentación se especifican a continuación en orden lógico.

- Codificación.- las medidas tomadas son almacenadas usando representaciones estandarizadas, generalmente denotadas en términos estadísticos o realizando una comparativa respecto al tiempo.
- Tabulación.- Los datos tomados serán tabulados de acuerdo al contexto obtenido, las herramientas de análisis de red como Moloch y Zabbix cuentan con sus propias bases de datos y visualización, también se clasifica los logs de INetSim según fecha de obtención de datos.
- Clasificación.- la información se clasificará posteriormente en diferentes tablas comparativas a estudiar, como; datos tomados previo a la infección, cambios posteriores en el sistema y red a la ejecución del malware. Se empleará herramientas de análisis estadísticos.

3.8. Recursos Humanos y Materiales

3.8.1. Recursos Humanos

- Autor:

  Orlando Jesús Brito Casanova.

- Director de Proyecto:

  Msc. Ing. Paulo Esteban Chiliguano Torres (hasta 30/09/18)

  Msc. Ing. Emilio Zhuma Mera.

- Docentes: Pertenecientes a la Facultad de Ciencias de Ingeniería (F.C.I) de la Universidad Técnica Estatal de Quevedo (U.T.E.Q).

3.8.2. Recursos Materiales.

3.8.2.1. Hardware.

Tabla 3: Recursos Hardware empleado.

CANTIDAD	EQUIPO	DESCRIPCIÓN
1	Computadora portátil.	Hp Pavilion 15r210dx • Intel® Core™ I5-5200U 2.20 GHz – 4 núcleos • 698.7 GB de disco duro • 4 GB de RAM
1	Computadora portátil. (empleada como servidor de virtualización)	Hp Pavilion 15r210dx • Intel® Core™ I5-5200U 2.20 GHz – 4 núcleos • 698.7 GB de disco duro • 8 GB de RAM
1	Router doméstico (Salida real a internet)	Cisco Linksys E1200
1	Impresora	Epson L210 con sistema de tinta continua.

Fuente: La Investigación
Elaborado por: Autor

3.8.2.2. Software.

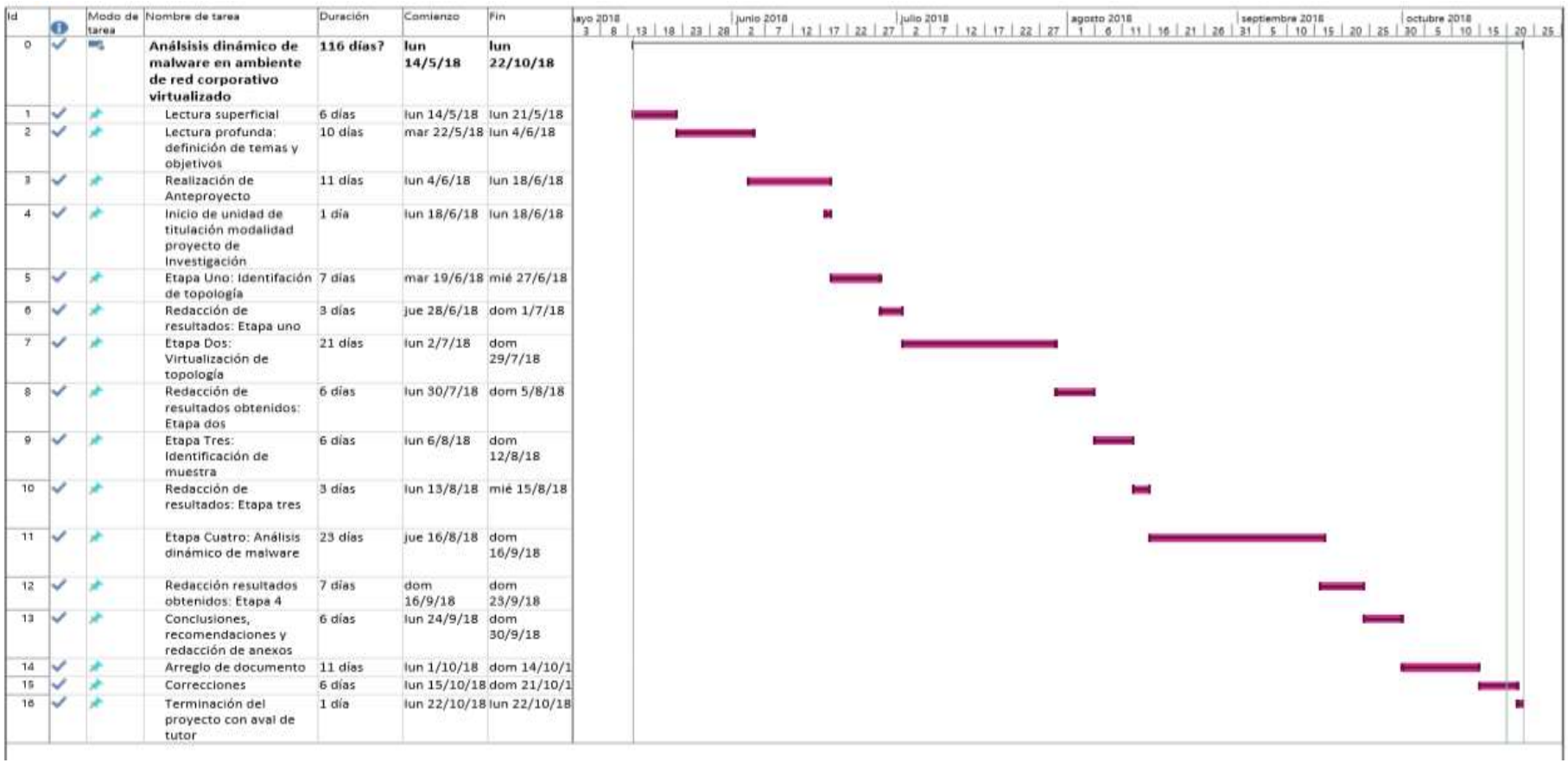
Tabla 4: Recursos Materiales y software empleado

NOMBRE	DESCRIPCIÓN
Proxmox 5.2	Software empleado para la creación de topología de redes virtuales.
Diversidad de malwares	Facilitados por organizaciones con fines de investigación (Hybrid-Analysis, Pupy)
Pupy	Herramienta de acceso remoto (RAT) con potencial capacidad para generación de software con fines pocos éticos.
Inetsim	Simulador de protocolos comunes de Internet. Permite el mejor aislamiento de la topología virtual.
Moloch	Capturador de paquetes y visualizador, en conjunto con ElasticSearch, posibilita el estudio profundo de los paquetes y conexiones establecidas.
Zabbix	Herramienta para graficar el rendimiento y consumo de recursos internos de los distintos equipos.
Daemonlogger	Demonio con capacidad de duplicar paquetes cursados por una red vitual y enviarlo a otra.
Imágenes de sistemas operativos	Definidos en la primera etapa correspondiente al estudio de topologías

Fuente: La Investigación
Elaborado por: Autor

3.9. Cronograma de Actividades

Ilustración 18: Cronograma de Actividades



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
0		**Análsisis dinámico de malware en ambiente de red corporativo virtualizado**	**116 días?**	**lun 14/5/18**	**lun 22/10/18**
1		Lectura superficial	6 días	lun 14/5/18	lun 21/5/18
2		Lectura profunda: definición de temas y objetivos	10 días	mar 22/5/18	lun 4/6/18
3		Realización de Anteproyecto	11 días	lun 4/6/18	lun 18/6/18
4		Inicio de unidad de titulación modalidad proyecto de Investigación	1 día	lun 18/6/18	lun 18/6/18
5		Etapa Uno: Identifación de topología	7 días	mar 19/6/18	mié 27/6/18
6		Redacción de resultados: Etapa uno	3 días	jue 28/6/18	dom 1/7/18
7		Etapa Dos: Virtualización de topología	21 días	lun 2/7/18	dom 29/7/18
8		Redacción de resultados obtenidos: Etapa dos	6 días	lun 30/7/18	dom 5/8/18
9		Etapa Tres: Identificación de muestra	6 días	lun 6/8/18	dom 12/8/18
10		Redacción de resultados: Etapa tres	3 días	lun 13/8/18	mié 15/8/18
11		Etapa Cuatro: Análisis dinámico de malware	23 días	jue 16/8/18	dom 16/9/18
12		Redacción resultados obtenidos: Etapa 4	7 días	dom 16/9/18	dom 23/9/18
13		Conclusiones, recomendaciones y redacción de anexos	6 días	lun 24/9/18	dom 30/9/18
14		Arreglo de documento	11 días	lun 1/10/18	dom 14/10/1
15		Correcciones	6 días	lun 15/10/18	dom 21/10/1
16		Terminación del proyecto con aval de tutor	1 día	lun 22/10/18	lun 22/10/18

Fuente: La Investigación
Elaborado por: Autor

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. Resultados obtenidos en la ETAPA UNO: Identificación de Topología Corporativa

4.1.1. Introducción.

La elección de una topología de red empresarial juega un rol fundamental para el desarrollo en un laboratorio de análisis de malware, cuya complejidad depende del tamaño infraestructural y servicios brindados a la organización. En esta etapa de proyecto se define como diseño de red típico a una topología de seguridad perimetral empleando: zona desmilitarizada, red interna, firewall- router e Internet; de amplio uso entre empresas medianas, pequeñas o sucursales de una gran corporación, con posibilidades de abstracción a elementos básicos, conservando operatividad y posibilitando la virtualización del entorno.

4.1.2. Breve análisis de topologías empresariales.

La D.R.A.E[34] define como empresa a *"la unidad de organización dedicada a actividades industriales, mercantiles o de prestación de servicios con fines lucrativos"* [32], conformando el eje central de la economía mundial con un profundo impacto histórico, cultural y social, reconocido por el aclamado economista Joseph Alois Schumpeter (1883 – 1950) al declarar como "destrucción creativa" al proceso de invocación de las empresas y las implicaciones sobre su productividad, realzando la importancia de la incorporación de nuevo conocimiento al sector productivo [33].

El desarrollo en las tecnologías computacionales y en las telecomunicaciones en general es aplicable en la operatividad de las organizaciones, siendo un pilar fundamental en la productividad de las mismas, independiente del servicio prestado. En el presente proyecto se define como "Red Empresarial" a la infraestructura o distribución de equipos de telecomunicaciones e informáticos usados como soporte en el desarrollo laboral. Si bien existen diversos enfoques al calificar empresas u corporaciones, tales como: objeto de actividad (productora de bienes o prestadora de servicios), ámbito de actuación (local, nacional y multinacional), sector económico, propiedad (pública, privada y mixta) o forma jurídica (empresario individual y sociedades). La actual investigación emplea una clasificación por tamaño expuesta por Sridhar Iyer en su charla sobre *"Introducción a las Redes Empresariales"* [34].

[34] Diccionario de la Real Academia Española

4.1.3. Elección de topología.

Si bien el diseño topológico físico de una red empresarial depende del tamaño de la corporación así como los servicios prestado por su infraestructura, es necesario tomar a consideración los recursos requeridos para su completa virtualización; a mayor elementos virtualizados, más capacidad computacional es requerida. Con el objetivo de virtualizar una red completa común entre organizaciones, para elaborar un laboratorio de análisis de malware, es necesario la realización de estudios completos de topología lógica y física de la infraestructura de red empresarial, división de la misma en componentes, representación de cada componente en unidades elementales e implementación de políticas de seguridad y configuraciones análogas a la realidad. Se adopta las siguientes directrices para la definición de una topología virtualizable y la realización de un laboratorio de análisis de malware:

- Diseño de amplio uso entre organizaciones medianas, pequeñas y sucursales de grandes corporaciones.
- Componentes individuales cuyas características puedan ser abstraídas o representadas en un único elemento virtualizable.
- Posibilidad de aplicación de políticas de seguridad y configuraciones estándares.

Se opta por la utilización de una modesta topología de seguridad perimetral de amplio uso empleando una DMZ con un cortafuego en trípode (ver ***Anexo 3***), siendo abstracción de una red empresarial a nivel «mili», según la categorización por tamaño de Sridhar Iyer [9], adicionando una red de monitoreo. Los componentes generales son expuestos en ***Tabla 5*** junto a breve descripción.

Tabla 5: Componentes de topología de seguridad perimetral con DMZ

Componentes	**Descripción**
Red Interna	Intranet o red corporativa, cuenta con políticas de seguridad estrictas de accedo desde el exterior, y cierta grado de restricciones en su tráfico de salida.
DMZ	Puede brindar servicios (DNS, FTP, WEB, Correo Electrónico) a la red interna como a clientes remotos desde internet. Son muy expuestos a peligros de seguridad.
Firewall – Router	Realiza la filtración del tráfico según las políticas de seguridad establecidas para cada interfaz o subred, así como el encaminamiento (ruteo) de paquetes.

Internet	Red de redes, cuya infraestructura no pertenece a la organización y principal fuente de amenazas de seguridad.
Monitoreo	Mantiene estadísticas y registros del comportamiento de la red, tanto en conjunto, así como por componentes individuales

Fuente: La Investigación
Elaborado por: Autor

4.1.4. Abstracción de componentes y elección de Sistemas Operativos.

Siguiendo la estructura especificada en ***Tabla 5***, se busca abstraer funcionalidades de cada componente, representándolos en una entidad única. No es necesario la creación de una topología de gran tamaño; debido a los fines de la actual investigación es necesario representar una arquitectura funcional, con capacidades de empleo en análisis dinámico de software malicioso. No obstante, en caso de requerir un estudio de los componentes en forma individual, es factible la utilización de una mayor cantidad de elementos, siempre y cuando se cuente con recursos necesarios. **Anexo *4*** presenta una topología de red corporativa básica según Tom Cross [35], director de Security Research.

4.1.4.1. Componente Red Interna.

Corresponde a equipos conectados entre sí en un área geográficamente pequeña, con fines operativos, la componente red interna puede ir desde un par de computadoras interconectadas a varias redes LANs diferentes, según diversos departamentos de la organización; también pueden contar con servidores internos que brinden servicios de base de datos, monitoreo o servidor de archivos. Al ser una parte crucial de la operación empresarial, su seguridad toma una significación primordial, esto debido a los datos confidenciales (secretos corporativos) que en ella se transporta o la relevancia de los datos almacenados.

Gran parte de una red interna se encuentra compuesta por estaciones de trabajos (workstations) usualmente operadas por profesionales en áreas distintas a la informática y con desconocimientos de buenas prácticas de seguridad de información. El tener acceso a información clasificada, supone altos riesgos asociados de seguridad.

Según encuesta realizada por la «StatCounter Global Stats reports» entre agosto y septiembre de 2017, Microsoft Windows es la familia de distribuciones de software para computadores de escritorio, y laptops más requerida (ver **Anexo *5***), con un total de 36,22% del mercado. Esto se complementa con las estadísticas reflejadas en «netmarketshare.com»

(ver **Anexo *6***), ubicando a «Windows 7» como la versión líder con un 43,38% del mercado hasta Junio del 2018 por encima de la última distribución disponible («Windows 10» con un 32,08%). Por ello se decide abstraer la componente de red interna en una única estación de trabajo con sistema operativo «Windows 7», en representación de una red LAN corporativa típica.

4.1.4.2. Componente DMZ.

Una zona desmilitarizada es un *"un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red"* [36], puede estar conformada desde un único servidor físico, hasta una completa granja de servidores con tecnologías de virtualización, esto depende de los servicios brindados, el tamaño de la organización y la cantidad de peticiones recibidas. Las estadísticas mostradas por «w3techs.com» (ver **Anexo *7***) confirman el liderazgo de los sistemas operativos basados en el kernel Linux con un 40.4% del mercado, superior al 31,9% de utilización de Windows Server. Los datos tomados hasta junio del 2017 por la news.netcraft.com (ver **Anexo *8***), indican la importancia en el mercado del servidor web en Apache con un 45% del mercado el cual puede ser implementado en plataformas GNU/Linux, Windows y Macintosh.

Se opta por la utilización de CentOS como sistema operativo empresarial, debido a la popularidad de su distribución y gran aplicación en servidores y su filosofía de código abierto, el cual soporta la implementación de servicios: web con Apache HTTPD, SMTP con Round Cube, y servicios de carpetas compartidas en SAMBA.

4.1.4.3. Componente Firewall – Router.

Los equipos enrutadores encaminan el tráfico al destino, mientras los Firewalls realizan un análisis de los paquetes para permitir o denegar los mismos de acuerdo a las políticas de seguridad establecidas. Si bien pueden ser equipos dedicados, existen sistemas operativos que cumplen de buena manera las funciones antes descritas y otros complementos. La elección del elemento representativo a virtualizar se basa en opciones populares, por ello, se toma a consideración el ranking expuesto hasta junio de 2018 por «itcentralstation.com» (ver **Anexo *9***), sobre reseñas de firewalls más utilizados; con lo correspondiente a medianas empresas, la lista se encuentra liderada por Cisco ASA, seguido de FortiGate y Pfsense. Se opta la utilización de Pfsense como Router-Firewall por sus múltiples características y posibilidades, facilidad de instalación y el hecho de ser software libre (basado en FreeBSD).

4.1.4.4. Componente Internet.

Unos de los puntos cruciales en la elaboración de un laboratorio de análisis de malware, es el aislamiento completo del computador o red a estudiar, sobre todo en el comienzo de la investigación, cuando se cuenta con información escasa o nula sobre el comportamiento del malware. Como es señalado en [37], muy a menudo el código estudiado intenta el establecimiento de conexión con equipos remotos a través de internet, donde una conexión real podría alertar a los atacantes sobre las intenciones de realizar análisis o la posibilidad de servidores fuera de línea, con el consecuente cambio de comportamiento de la muestra estudiada. Se emplea conmutación entre tres diferentes topologías de acuerdo a las necesidades específicas y las características del malware a estudiar.

4.1.4.4.1. Conmutación con INetSIM.

Evaluar las comunicaciones del malware permite la obtención de información muy valiosa, y aplicando una suite de simulación de servicios comunes de internet asegura el aislamiento de la red y mayor prudencia en el análisis. Se elige INetSim (para plataformas Linux) como herramienta para generar respuestas falsas de varios protocolos usuales de internet, implementado en una máquina con sistema operativo Ubuntu.

4.1.4.4.2. Conmutación con RAT PUPY.

La herramienta de acceso remoto PUPY es una contribución desarrollada y distribuida en GITHUB, si bien posee fines tales como educación e investigación, puede usarse para crear código malicioso de acuerdo a especificidades de varios sistemas (Windows, Linux, MAC y Android) y servidor de control para los ambientes infectados. El servidor de PUPY se implementa en máquina virtual independiente con sistema operativo Ubuntu.

4.1.4.4.3. Conmutación con Internet real.

Necesario para malware con llamados a direcciones IP externas, donde su comportamiento está truncado al no recibir la información correcta. Es uno de los puntos más críticos al poner en evidencia la ubicación del investigador y vulnerar la red y privacidad del mismo, debe de emplearse en situaciones extremas, donde los datos obtenidos dentro de una topología completamente aislada, no son suficientes para entender el comportamiento ni los fines del código malicioso.

4.1.4.5. Componente Monitoreo.

Monitorear redes o sistemas tiene gran significancia con temas referentes a seguridad, solución de problemas, reasignación de recursos… En general, corresponde un ahorro de tiempo y dinero para las organizaciones por las diferentes posibilidades brindadas, tal como es mostrado en varias publicaciones [38], [39], [40].

El componente "Monitoreo" es abstraído de servidores y equipos enfocados a varias operaciones, tanto la recolección de registros, estudio de los paquetes transitados por la red, y la gráfica de rendimiento y uso de los componentes de estudio. Considerando la facilidad de instalación, características de software libre y correcto funcionamiento entre varios sistemas operativos (Windows, Linux) que conforman la red, se decide por la implementación de Moloch como analizador de paquetes principal y Zabbix como herramienta de monitoreo interno, implementados en S.O Ubuntu 18.04.1, ambas herramientas constan de su respectiva web-GUI[35], la cual puede ser accedida por un computador en red con el servidor de virtualización y conexión real a internet.

4.1.5. Tabla de resumen de elección de sistemas operativos y servicios por componentes.

Tabla 6: Sistemas Operativos por componente

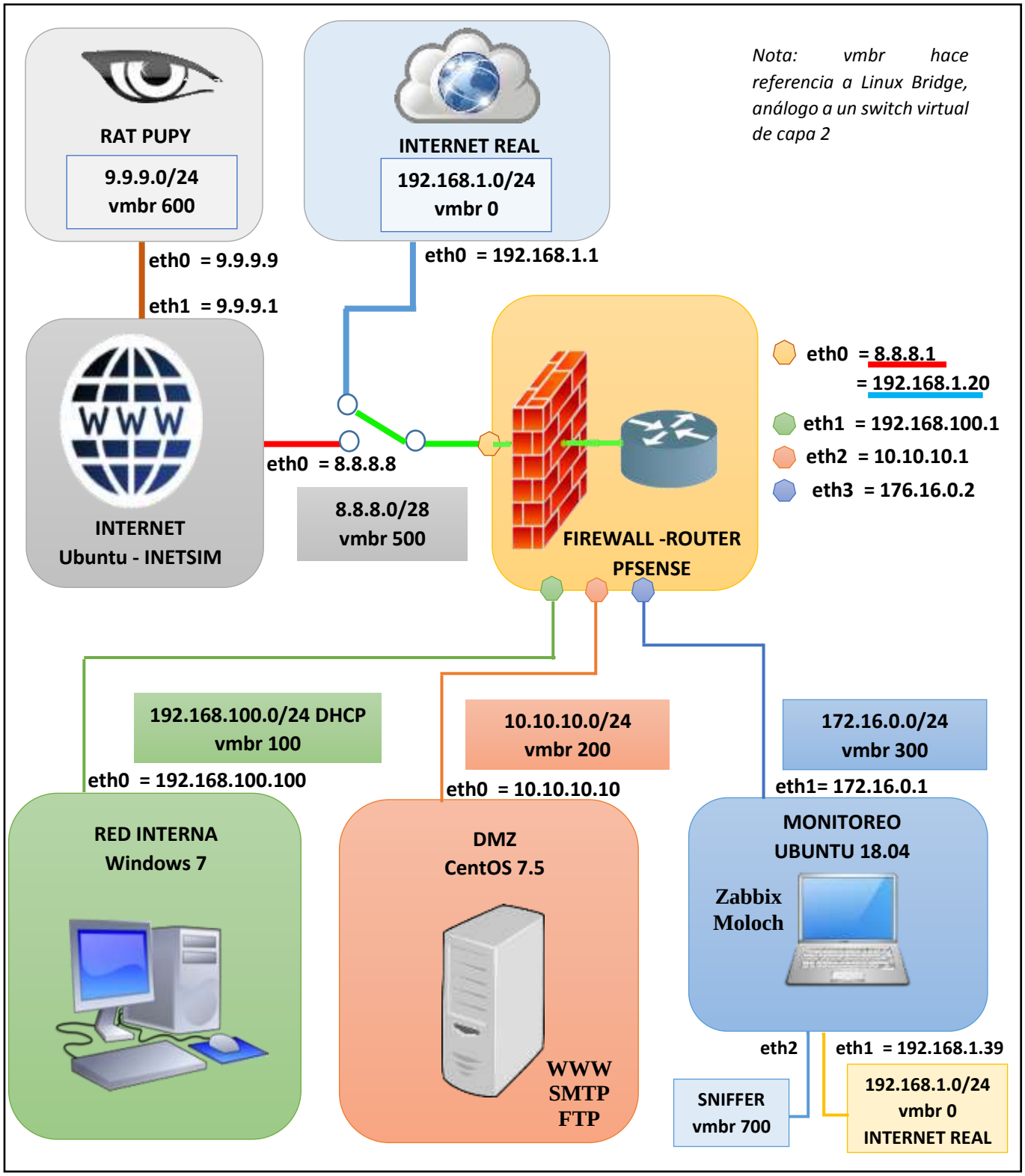
Componente	*Sistema Operativo*
Red Interna	Microsoft Windows 7 Ultimate Service Pack 1 64 bits
DMZ	CentOS Server 7.5 64 bits
Firewall-Router	Pfsense Community Edition 2.4.3 64 bits
Internet	• INetSim 1.2.8 released 2018-06-12 implementado en Ubuntu 14.04.2 • Rat PUPY implementado en Ubuntu 14.04.2 • Conectividad a router físico con salida a Internet real.
Monitoreo	Ubuntu 18.04.1 LTS 64 bits

Fuente: VirusTotal.com
Elaborado por: Autor

[35] Administración y control mediante página web contenida en servidor de la herramienta

4.1.6. Diseño y topología de red empresarial

Ilustración 19: Topología lógica de red empresarial a implementar



Fuente: La investigación
Elaborado por: Autor

4.2. Resultados obtenidos en la ETAPA DOS: Virtualización de Topología.

4.2.1. Introducción.

El establecimiento de un entorno aislado juega un rol importante para el desarrollo de análisis dinámico de manera segura, cual puede enfocarse desde un solo computador, hasta al estudio de una topología de red completa física o virtualizada. En este punto se define las características de red a virtualizar, la abstracción de sus diferentes componentes en únicos elementos con el fin de salvaguardar los recursos, la creación e instalación de los sistemas operativos correspondiente y las configuraciones necesarias para una red completamente operativo y funcional.

4.2.2. Elección de plataforma de virtualización.

"La virtualización es la combinación entre ingeniería de hardware y software para la creación de máquinas virtuales (VM) permitiendo a múltiples sistemas operativos ser ejecutados en la misma plataforma física" [41], forma parte de las tecnologías con un gran impacto en la actualidad por sus múltiples ventajas y nuevas posibilidades; permite el rápido escalamiento, es primordial en la existencia de la computación en la nube, posibilita mayor flexibilidad y el pago únicamente por los recursos usados.

Al momento de elegir el software o plataforma de virtualización es importante conocer las tipos y arquitecturas existentes y realizar una evaluación de los requerimientos necesarios para el desarrollo de un laboratorio de análisis de malware. Para ello se ha establecido las siguientes directrices:

- Utilización óptima recursos hardware del computador.
- Facilidades en la interconexión de máquinas virtuales y la creación de un entorno aislado.
- Conservación de rendimiento con ejecución de varias máquinas virtuales de forma simultánea.

Tabla 7 resume las características de virtualización seleccionadas según directrices mencionadas con anterioridad para la definición de una plataforma de virtualización, según clasificación realizada por tipo (almacenamiento, servidor, red, memoria, aplicación, plataforma –hardware y desktop), técnica (virtualización de OS, emulación de hardware y paravirtualización) y arquitectura (hipervisor y Host OS).

Tabla 7: Elección de tipo, técnica y arquitectura de virtualización

Clasificación	*Elección*	*Descripción*
Tipo	**Virtualización de servidor**	Permite la ejecución y el compartimiento de recursos hardware entre diferentes sistemas operativos simultáneos y el acceso a usuarios remotos.
Técnica	**Virtualización completa**	Emplea técnicas para crear instancias de un entorno, la imagen binaria del sistema operativo se manipula en el tiempo de ejecución y el código de nivel de usuario se ejecuta directamente en el procesador para virtualización de alto rendimiento. [41]
Arquitectura	**Hipervisor**	(ver **Anexo *10***) Permite que varios S.O. se ejecuten simultáneamente en un solo host físico, así como, proporciona abstracción de hardware al SO huésped (Guest OS) y multiplexa de manera eficiente los recursos de hardware subyacentes. [41]

Fuente: La investigación
Elaborado por: Autor

4.2.3. Elección de plataforma de virtualización, características y diferencias con softwares similares.

Existen variedad de opciones con respecto a plataformas y software de virtualización, tanto de código abierto como de pago, algunos muy usados en áreas investigativas y otros con aplicaciones en la industria. «trustradius.com» (ver **Anexo *11***) muestra estadísticas de frecuencia de investigación para softwares de virtualización de servidores, en los que sobresalen VMWare ESXi (20.1%), seguido por Proxmox (18.4%) y Oracle VirtualBox (11,6%) y demás plataformas.

Siguiendo las directrices mencionadas en la sección ***4.2.2*** y lo estipulado en ***Tabla 7***, es seleccionada Proxmox VE en su versión 5.2 como plataforma de virtualización, al contar con características que facilitan el monitoreo tanto del entorno completo como de cada elemento independiente, con posibles aplicaciones en análisis dinámico de malware. Otras particularidades a resaltar son: versatilidad, estabilidad, confiabilidad, velocidad al usar dos

tecnologías de virtualización populares (KVM y LXC) y su filosofía de software libre; es de muy fácil instalación y configuración (basado en Debian) y posee una interfaz WEB intuitiva y amigable con el usuario.

Esta elección contrasta con los softwares de virtualización más usados para el levantamiento de un laboratorio de análisis de malware como VMWare Workstation PRO y Oracle VirtualBox; la decisión está basada de acuerdo a las posibilidades brindadas inclusive sin subscripción alguna y ser un hipervisor completo, lo cual aprovecha el hardware de un servidor dedicado a virtualizar el entorno.

4.2.4. Recursos necesarios para implementación de topología.

Se detalla los requisitos mínimos de hardware para los distintos componentes que conforma el laboratorio de análisis para establecer una correcta distribución de los recursos de la máquina host.

4.2.4.1. Tabla de requerimiento mínimo y recoRemendable para Proxmox.

Información obtenida en la wiki oficial pve.proxmox.com [42].

Tabla 8: Requerimientos mínimos y recomendaciones de PROXMOX

	Mínimo	***Recomendado***
CPU	64bit (Intel EMT64 or AMD64)	64bit (Intel EMT64 or AMD64), se recomienda múltiples núcleos
Tecnología de virtualización	Intel VT/AMD-V capable CPU/Mainboard for KVM Full Virtualization support	Intel VT/AMD-V capable CPU/Mainboard for KVM Full Virtualization support
RAM	1 GB (únicamente para el host)	8 GB
Disco Duro	Sin importancia	Mejores resultados con 15k rpm SAS, Raid10
Tarjetas de red	1	Al menos 2

Fuente: La investigación
Elaborado por: Autor

4.2.4.2. Tabla de requerimientos mínimos por sistema operativo.

Tabla 9: Requerimientos mínimos por sistema operativo

Requerimiento	*Windows 7*[36]	*Ubuntu 14.04*[37]	*CentOS 7.5*[38]	*PFSENSE*[39]
CPU	1 GHz	300 MHz	300 GHz	500 MHz
RAM	1 GB	225 Mb	1 GB	512 Mb
Disco Duro	20 GB	1,5 GB	2 GB	1 GB
Tarjeta de Red	-	-	-	Mínimo 2

Fuente: La investigación
Elaborado por: Autor

4.2.4.3. Tabla de recursos disponibles y su distribución entre distintos componentes.

El rendimiento de la topología ejecutada simultáneamente depende de las capacidades disponibles respecto a recursos hardware del servidor físico donde se implemente, es por ello de primordial importancia una correcta distribución de los recursos, garantizando los requerimientos mínimos de cada sistema operativo individualmente para posibilitar el desarrollo de un laboratorio de análisis veloz. ***Tabla 10*** muestra la definición de los recursos para cada componente así como las características hardware del servidor físico.

Tabla 10: Distribución de recursos

	CPU	*Disco duro*	*RAM*	*Tarjeta de red*
Servidor Físico (Hp Pavilion 15r210dx)	Intel® Core™ I5-5200U 2.20 GHz – 4 núcleos	698.7 GB	8 GB	1
Windows 7	2 núcleos	32 GB	1 GB	1
CentOS 7.5	2 núcleos	32 GB	1 – 3 GB	1
Ubuntu 14.04	2 núcleos	32 GB	1 GB – 1GB(swap_	1
Pfsense 5.2	2 núcleos	32 GB	1 – 3 GB	3

Fuente: La investigación
Elaborado por: Autor

[36] http://windows7.windowsreinstall.com/systemrequirements.htm
[37] https://help.ubuntu.com/community/Installation/SystemRequirements
[38] https://access.redhat.com/documentation/en-us/red_hat_directory_server/9.0/html/installation_guide/platform_support
[39] https://www.pfsense.org/products/

4.2.5. Creación e instalación de Máquinas Virtuales.

4.2.5.1. Obtención de Imágenes «.iso».

Una imagen «.iso» *es "una copia exacta del sistema de archivo de un CD-ROM o DVD guardada siguiendo el formato ISO-9660"* [43] siendo esta junto con memorias USB los principales medios de instalación. En ***Tabla 11*** se describen las fuentes y particularidades en la adquisición de archivos «.iso» necesarios para instalación de los elementos a usar. La obtención de Ubuntu establecido como elemento abstracto del componente Internet se detalla en punto posterior, al diferenciarse este del tipo de tecnología virtualización usada en los demás casos.

Tabla 11: Fuentes de Imágenes ISO

	Fuente	***Descripción***
PROXMOX 5.2	Proxmox.com[40]	Proxmox Virtual Enviroment se encuentra publicado bajo licencia GNU AGPL, V3, siendo su descarga, uso y compartición totalmente gratuita. No obstantes cuenta con diferentes tipos de suscripciones por servidor físico y cpu para empresas, brindando un mayor soporte y capacidades de actualización.
Windows 7	Microsoft.com[41]	Al ser un sistema operativo bajo licencia comercial, se opta por la descarga de una prueba de 90 días, tiempo suficiente para el desarrollo de la investigación.
CentOS 7.5	Centos.org[42]	Al ser software libre y gratuito, su descarga se simplifica al ingreso de la página oficial y en la elección del «.iso» conveniente, se elige el modo "Everything ISO", cual proporciona todos los recursos en un solo archivo (8.8 GB)

[40] https://www.proxmox.com/en/downloads/category/iso-images-pve
[41] https://www.microsoft.com/es-es/download/details.aspx?id=5842
[42] https://www.centos.org/download/

Pfsense 2.4.3	Pfsense.org[43]	Es de código abierto por lo que su obtención es totalmente gratuita, pero es necesario la especificación de versión, medio de instalación y arquitectura de CPU (ver **Anexo *12***)

Fuente: La investigación
Elaborado por: Autor

4.2.5.2. Instalación de PROXMOX VE.

Proxmox Virtual Enviroment es de muy fácil instalación, inclusive puede ser actualizado desde una máquina Debian previamente instalada. A continuación se resalta los hechos de significancia durante la instalación del mencionado hipervisor:

- Antes de proceder con la instalación es requerido la preparación del equipo físico a implementarse, los recursos debe de ser los suficientes para permitir la creación y ejecución simultánea de varias máquinas virtuales; además, como es indicado en [44], se necesita de la habilitación de capacidades de virtualización de nuestro CPU (Intel VT-x o AMD-V), este proceso se lo configura en la BIOS de la mainboard, para lo cual se requiere cortar el proceso de arranque.
- Se debe de preparar el medio contendor de la imagen «.iso» para la instalación, en el caso de usar pendrive USB es necesario considerar los programas usados para conversión a un USB booteable[44] (no funciona con UNetbootin or Rufus), como es indicado en [45], es preferente el uso de «etcher» en el flasheo del dispositivo.
- El proceso de instalación es gráfico e intuitivo, pasando desde el formato del disco (se emplea todo el espacio disponible) hasta la configuración regional y direccionamiento IP. Se recomiendo precaución con la ip configurada, debido a que la misma es usada en el acceso a la WEB GUI de Proxmox mediante el protocolo HTTPS por defecto al puerto 8006, si es necesario una reconfiguración del direccionamiento ip, se lo puede realizar mediante la consola de administración o la mediante web, al estar basado en Debian se puede modificar el archivo '/etc/network/interfaces' en la sección de vmbr0, la cual es un puente para la interfaz física (enp8s0) y via web en la sección '/System/Network'.

[43] https://www.pfsense.org/download/
[44] Capacidad de un medio para auto ejecutarse sin necesidad de Sistema Operativo alguno.

4.2.5.3. Creación de Bridges.

Un puente (bridge) es una abstracción de un switch de capa dos implementado en software, todas las máquinas virtuales pueden compartir un único puente o separar los dominios de diferentes máquinas virtuales mediante la aplicación de varios puentes. La analogía de switch hace posible la creación de una red aislada, así como la interconexión entre equipos, como indica [46], la correcta notación para los bridge es vmbr[N] en donde 0<N<4094, es preciso señalar que desde la versión 5.0 la terminología «eth0» quedó en desuso para las interfaces físicas (NIC), siendo remplazada por el prefijo «en».

En proxmox la creación de un Linux bridge es relativamente fácil, una vez señalado el nodo a configurar, se procede a la búsqueda de la sección 'System/Network' que muestra todas las interfaces disponible para posteriormente dentro de menú pertinente escoger 'Create – Linux Brige'. Para efectos de aislación de red, únicamente se configura el nombre del puente, según la relación establecida en ***Tabla 12***. En ***Ilustración 20*** muestra la configuración de red para el nodo principal de proxmox.

Tabla 12: Función de los diferentes VMBR a usarse

VMBR	***Función***
0	Se encarga de la conexión con nuestra red LAN, permite el acceso a la WEB GUI, tiene como puente la NIC enp8s0. Consta con salida a internet.
100	Switch virtual para interconexión de componentes de red interna (Firewall eth1 – Intranet 7 eth0)
200	Switch virtual de interconexión para componente DMZ (Firewall eth2 – DMZ eth0)
300	Switch virtual establecido para la red de "Monitoreo" (Firewall eth3 – Monitoreo eth1)
600	Switch virtual para interconexión de entre servidor INetSim y RAT Pupy
500	Posibilita la interconexión entre los componentes que simularán Internet (Firewall eth0 – Inetsim eth0)
700	Con la correcta configuración de eth2 de Monitoreo y uso del demonio "daemonlogger", se obtiene el funcionamiento de un HUB, posibilitando la escucha de paquetes de varias redes.

Fuente: La investigación
Elaborado por: Autor

Ilustración 20: Implementación de Linux Bridge

Name	Type	Active	Autostart	VLAN a...	Ports/...	IP address	Subnet mask	Ga	Comment
enp8s0	Network Device	Yes	No	No					
vmbr0	Linux Bridge	Yes	Yes	No	enp8s0	192.168.1.254	255.255.255.0	192.	Internet real
vmbr100	Linux Bridge	Yes	Yes	No					RED INTERNA
vmbr200	Linux Bridge	Yes	Yes	No					DMZ
vmbr300	Linux Bridge	Yes	Yes	No					Monitoreo
vmbr500	Linux Bridge	Yes	Yes	No					INTERNET (Simulacion)
vmbr600	Linux Bridge	Yes	Yes	No					PUPY
vmbr700	Linux Bridge	Yes	Yes	No					SNIFFER
wlp9s0	Unknown	No	No	No					

Fuente: La investigación
Elaborado por: Autor

4.2.5.4. Elección de tecnologías de virtualización según componentes.

Proxmox virtualiza elementos usando dos tecnologías, cuales poseen cualidades diferentes haciéndolas indicadas para cierto tipo de máquina virtual según los requerimientos. Estas tecnologías son: LXC (usado en la implementación de containers[45] «CT»), permite la ejecución de un sistema operativo completo dentro del núcleo del hipervisor, esto limita las capacidades, restringe su uso a sistemas operativos de núcleo Linux, pero, permite un mejor ahorro de recursos (CPU, RAM); QEMU/KVM (usado en implementación de VM), emula un computador físico con sus recursos, particiones, archivos, tarjetas de red, como si fuera un dispositivo real.

En ***Tabla 13*** se presenta la elección de sistema de virtualización para los componentes de la red empresarial con su respectiva justificación.

Tabla 13: Elección de sistema de virtualización (CT - VM)

Sistema	*Elementos*	*Justificación*
CT (LXC)	Ubuntu 14.04 para implementación de servicio INetSim, servidor Pupy y de Monitoreo	La creación de un container limita las capacidades pero optimiza los recursos, esta tecnología puede ejecutar procesos de pocos requerimientos, por ello se decide su utilización para el levantamiento del servicio INetSim (emulación de Internet), TT Pupy (herramienta de acceso remota), e implementación de un servidor de monitoreo con los servicios Moloch y Zabbix.

[45] Alternativa ligera a virtualización completa

VM (Qemu/KVM)	Windows 7, PFsense y CentOS	Divide los recursos para cada dispositivo ejecutado, incrementado considerablemente la carga de cpu y el uso de memoria RAM, pero permite la creación de máquinas virtuales con kernel diferentes de Linux como «Windows 7» y «Pfsense» (FreeBSD); no obstante es empleada en la creación de la red DMZ al brindar mayor aislamiento e independencia del sistema hipervisor.

Fuente: La investigación
Elaborado por: Autor

El proceso de creación y obtención de los recursos de instalación difiere entre estos dos sistemas de virtualización; VM trabaja directamente con imágenes «.iso» descargadas de diferentes fuentes, estas son subidas directamente al storage local de proxmox; en cuanto se refiera a CT, es necesario la obtención de templates LXC, los mismos que pueden ser obtenidos desde el propio proxmox y no requieren del proceso de instalación del sistema operativo. En ***Ilustración 21***, ***Ilustración 22***, ***Ilustración 23***, ***Ilustración 24*** *e* ***Ilustración 25*** muestran los recursos implementados en la creación de las máquinas virtuales.

Ilustración 21: Hardware implementado para elemento VM Windows 7

Keyboard Layout	Default
Memory	1.00 GiB
Processors	2 (1 sockets, 2 cores)
Display	Default
Hard Disk (ide0)	local-lvm:vm-203-disk-1,size=32G
CD/DVD Drive (ide2)	local:iso/Win7UltiSP1_64Bits_SteveTutoriales.iso,media=cdrom
Network Device (net0)	rtl8139=BA:D8:C3:67:56:A4,bridge=vmbr100
USB Device (usb0)	spice

Fuente: La investigación
Elaborado por: Autor

Ilustración 22: Hardware implementado para elemento VM CentOS

Keyboard Layout	Default
Memory	1.00 GiB/3.00 GiB
Processors	4 (2 sockets, 2 cores)
Display	Default
CD/DVD Drive (ide2)	local:iso/CentOS-7-x86_64-DVD-1804.iso,media=cdrom
Hard Disk (scsi0)	local-lvm:vm-250-disk-1,size=32G
Network Device (net0)	rtl8139=AA:D7:90:0F:AD:5A,bridge=vmbr200

Fuente: La investigación
Elaborado por: Autor

Ilustración 23: Hardware implementado para elemento VM PFsense

Keyboard Layout	Default
Memory	1.00 GiB/3.00 GiB
Processors	2 (1 sockets, 2 cores)
Display	Default
CD/DVD Drive (ide2)	local:iso/pfSense-CE-2.4.3-RELEASE-amd64.iso,media=cdrom
Hard Disk (virtio0)	local-lvm:vm-200-disk-1,size=32G
Network Device (net0)	virtio=02:1F:1D:E4:47:51,bridge=vmbr500
Network Device (net1)	rtl8139=EE:D7:5E:6D:C6:01,bridge=vmbr100
Network Device (net2)	rtl8139=EA:D8:87:E6:70:01,bridge=vmbr200

Fuente: La investigación
Elaborado por: Autor

Ilustración 24: Recursos implementados en CT Internet – Ubuntu

Memory	1.00 GiB
Swap	1.00 GiB
Cores	2
Root Disk	local-lvm:vm-5000-disk-1,size=32G
Mount Point (mp0)	/mnt,mp=/mnt

Fuente: La investigación
Elaborado por: Autor

Ilustración 25: Recursos y redes implementados en CT Monitoreo – Ubuntu

ID	Name	Bridge	Firewall	VLAN T...	MAC address	IP address	Gateway
net0	eth0	vmbr0	No		EA:A3:EF:B...	192.168.1.39/24	192.168.1.1
net1	eth1	vmbr300	No		92:C0:92:06...		
net2	eth2	vmbr700	No		5A:CE:D2:6...		

Memory	4.00 GiB
Swap	2.00 GiB
Cores	4
Root Disk	local-lvm:vm-7000-disk-1,size=120G

Fuente: La investigación
Elaborado por: Autor

4.2.5.5. Instalación de sistemas operativos.

Una vez creada las VM y CT correspondiente a cada componente definido en la topología de red empresarial para la creación de un laboratorio de análisis de malware, procede la instalación de los elementos que así lo requieran, para ello se deben de tener a consideración los recursos definidos para cada máquina virtual. En la ***Tabla 14*** se realiza una descripción breve de los hechos sobresalientes en la instalación de cada S.O.

Tabla 14: Breve descripción de instalación para los S.O requeridos

Elemento	*Sistema de virtualización*	*Descripción de Instalación*
Windows 7	VM	Instalación típica de versión de prueba (90 días) al no contar con licencia de activación.
CentOS 7.5	VM	Instalación gráfica, donde sobresale la implementación del grupo de paquete "Servidor con interfaz gráfica de usuario" para el levantamiento de una GUI.
Pfsense 5.2	VM	Instalación típica con AUTO (UFS) para particionamiento del disco.
Ubuntu 14.04	CT	No requiere instalación alguna al provenir de un template obtenido mediante repositorios libres de Proxmox.

Fuente: La investigación
Elaborado por: Autor

4.2.6. Configuraciones e implementación de red empresarial.

4.2.6.1. Configuración de INETSIM (Componente Internet).

Antes de proceder a la descarga e instalación de la suite «INETSIM» para Ubuntu se prepara el entorno; establecer vmbr0 como puente, para de esta manera poseer acceso a internet; es necesario la instalación de los requerimientos como prerrequisitos para el correcto funcionamiento del software (ver ***Anexo 13*****)**, donde el paquete '*libiptables-ipv4-ipqueue-perl*' no cuenta con disponibilidad para Ubuntu y al ser este opcional [47] se obvió su instalación.

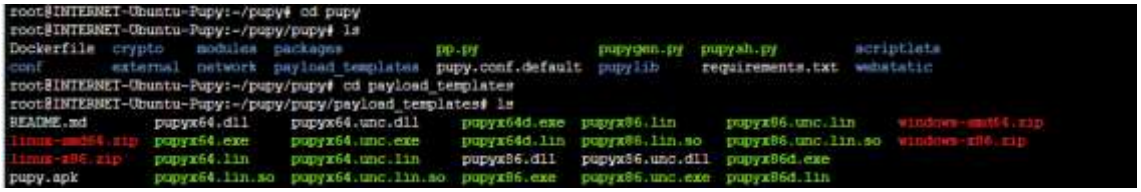
Para realizar la descarga mediante la herramienta «apt», es requerido actualizar la lista de repositorios, este se realiza agregando la línea *'deb http://www.inetsim.org/debian /binary'* en el archivo *'/etc/apt/sources.list'* y descargar la llave necesaria *'wget -O - http://www.inetsim.org/inetsim-archive-signing-key.asc | apt-key add -'*; después de la actualización de los repositorios *'apt-get update',* procede su descarga e instalación *'apt-get install inetsim'*. Para este punto es necesario el establecimiento como puente de la interfaz a vmbr500.

Una vez instalado es necesario realizar ciertas configuraciones, primero disponer del inicio automático de los servicios con el arranque del sistema operativo, establecer '*ENABLED = 1'* en *'/etc/default/inetsim'*. El archivo de configuración principal es *'/etc/inetsim/inetsim.conf*', donde se establece los siguientes parámetros *'service_bind_adress 8.8.8.8', 'dns_defaul_ip 8.8.8.8'* (Nótese la dirección ip configurada en la interfaz) y '*dns_default_domainname orlandbri.com'*. Al guardarse los cambios se debe de reiniciar el servicio *'service inetsim restart'*.

4.2.6.2. Implementación de RAT PUPY.

La herramienta de acceso remoto (RAT) «Pupy» provee distintas funcionalidades para generación de software, conociendo características del sistema objetivo, puede desarrollar código malicioso con capacidad de tomar control absoluto de la máquina víctima. Para su implementación en contenedor virtual con Ubuntu 14.04, es necesario la instalación del paquete 'git' para la clonación del repositorio, y demás paquetes basados en python para la ejecución correcta del servicio (ver **Anexo *14***). ***Ilustración 26*** presenta el directorio "pupy".

Ilustración 26: Directorio /root/pupy/pupy



Fuente: VirusTotal.com
Elaborado por: Autor

4.2.6.3. Configuración de PFSENSE (Componente Firewall – Router).

Pfsense cuenta con una interfaz de configuración web intuitiva, cual puede accederse mediante direccionamiento IP configurado para su interfaz LAN (eth1). Las configuraciones iniciales deben realizarse directamente desde la terminal, mediante un menú de opciones básico, de esta manera empleando la opción 1, se asigna las funcionalidades a las diferentes interfaces creadas, agregándose la interfaz opt1 la cual será usada por la DMZ y opt2 perteneciente a red Monitoreo, posterior a la asignación procede la configuración de direccionamiento IP por interfaz. La ***Ilustración 27***, muestra el direccionamiento y la asignación implementada. «opt1» y «opt2» están denotadas por 'DMZ' y 'MONITOREO' respectivamente, cambio realizado mediante interfaz WEB.

Ilustración 27: Direccionamiento IP y asignación de interfaz pfsense

Fuente: La investigación
Elaborado por: Autor

El acceso a la WEB GUI es realizado usando la VM «Windows 7» ubicada en la componente LAN, con direccionamiento IP estático inicialmente con el Gateway correspondiente la interfaz LAN de pfsense. Mediante https y la dirección 192.168.100.1 (agregando la respectiva excepción en el navegador Mozilla), se ingresa al login del sistema cuyas credenciales por defectos son admin y pfsense (por cuestiones de seguridad es recomendable su cambio) para el usuario y contraseña respectivamente.

La componente Firewall-Router se encarga de cumplir varias funciones, como, servidor DHCP para red «LAN», traducción de direcciones de red (NAT) para salida de las redes internas a la interfaz «WAN», firewall con reglas definidas por interfaces, DNS resolver para el servidor DMZ.

En la sección ´Services/DHCP Server/ LAN´ es habilitado el servicio DHCP con los parámetros indicado en ***Ilustración 28***, cabe resaltar que se distribuirá dos direcciones para servidores DNS, el primario (192.168.100.1) que corresponde al servicio DNS resolver de pfsense y el secundario (8.8.8.8) correspondiente a InetSim.

Ilustración 28: Configuración de servidor DHCP

Fuente: La investigación
Elaborado por: Autor

Para la resolución de direccionamiento IP dirigido hacia el servidor que presta servicio WEB en la zona desmilitarizada, es empleado el servidor «DNS Resolver», cuya configuración se realiza en ‘Services/DNS Resolver/General settings’ agregando lo mostrado en ***Ilustración 29***, lo cual al recibir una petición dns (puerto 53) para los dominios determinados devuelve una dirección ip correspondiente.

Ilustración 29: Configuración de DNS resolver, pfsense

Fuente: La investigación
Elaborado por: Autor

«NAT» es empleado para traducir direcciones IP o puertos, obligatorio cuando se cuenta con redes privadas y acceso al internet, debido a que los routers de los proveedores descartan los rangos de direcciones establecidos en la «RFC-1918», para el nateo del servidor DMZ se usa la funcionalidad «1:1», cual asigna una dirección IP pública específica a dicho host (configuración realizada en 'Firewall/NAT/1:1', mostrado en ***Ilustración 30***); por otra parte se usa nateo manual outbound para permitir la salida de equipos conectado en la red LAN empleando la dirección IP del puerto WAN (configuración realizada en 'Firewall/Nat/Outbound', mostrada en ***Ilustración 31***).

Ilustración 30: Nateo 1:1 para componente DMZ

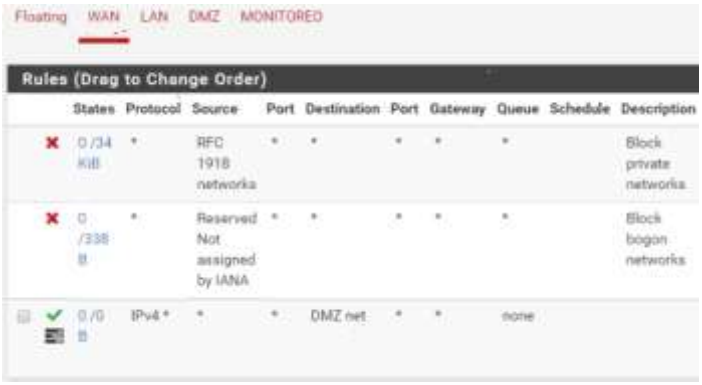
Fuente: La investigación
Elaborado por: Autor

Ilustración 31: Nateo manual Outbound para compoente LAN

Fuente: La investigación
Elaborado por: Autor

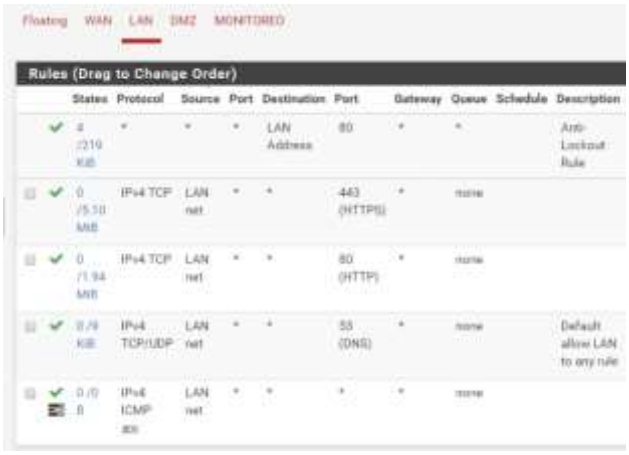
Con lo correspondiente al Firewall, se realiza una configuración implementando políticas de seguridad estándares para redes internas y zonas desmilitarizadas siguiendo lo recomendado en [48], la configuración es desarrollada en "Firewall/rules" y se diferencia para cada interfaz. En ***Ilustración 32***, ***Ilustración 33***, ***Ilustración 34*** e ***Ilustración 35*** muestran las reglas establecidas.

Ilustración 32: Reglas para interfaz WAN, pfsense



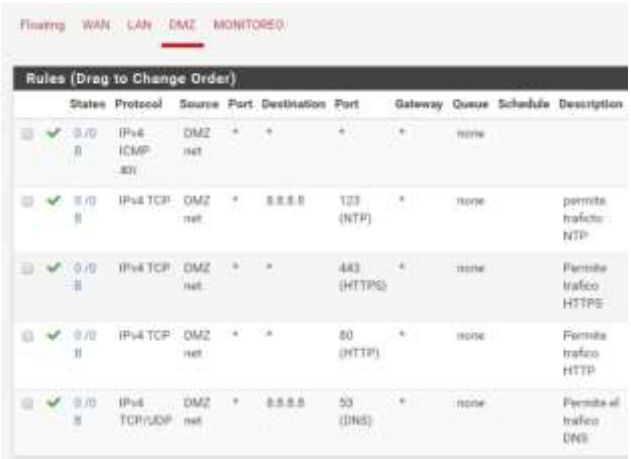
Fuente: La investigación
Elaborado por: Autor

Ilustración 33: Reglas para interfaz LAN, pfsense



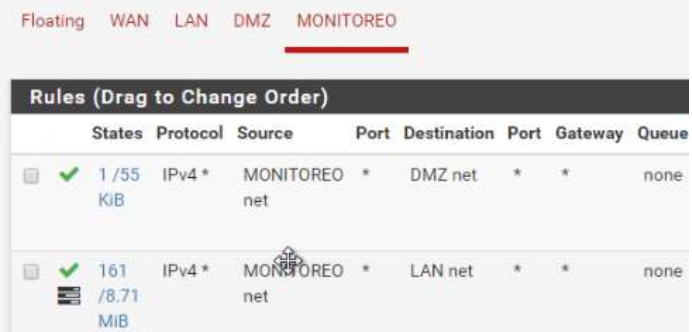
Fuente: La investigación
Elaborado por: Autor

Ilustración 34: Reglas para interfaz DMZ, pfsense



Fuente: La investigación
Elaborado por: Autor

Ilustración 35: Reglas para interfaz MONITOREO, pfsense



Fuente: La investigación
Elaborado por: Autor

4.2.6.4. Levantamiento de servicios en componente DMZ.

- **Servidor web Apache.**

El procedimiento de configuración y archivos necesarios para el levantamiento de una página web http sencilla, se describe en el manual expuesto en **Anexo *15***. Para tener acceso a la web desde el exterior, es necesario agregar la siguiente regla *'# firewall-cmd --zone=public --add-port=80/tcp –permanent'*. ***Ilustración 36*** muestra la página web accedida desde el componente red interna.

Ilustración 36: Página web alojada en DMZ

Fuente: La investigación
Elaborado por: Autor

- **Servidor de correos.**

Común dentro de los servicios corporativos, se cuenta con la aplicación de un servidor SMTP y el protocolo IMAP4 para conservar los correos electrónicos de varios clientes, cuales puedan acceder a los mismos mediante el web-mail RoundCube.

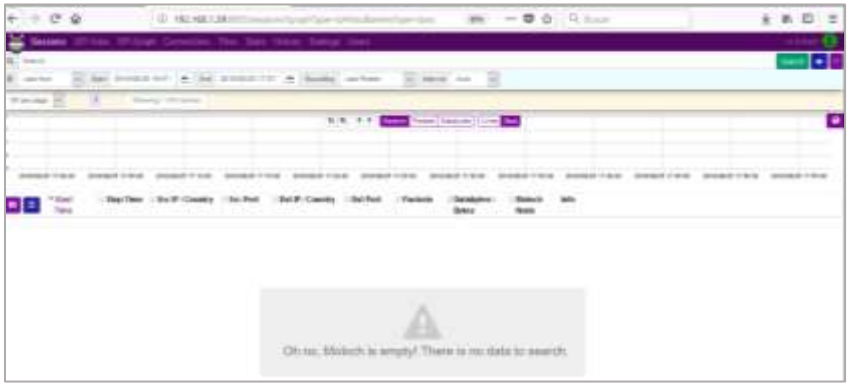
- **Servidor de archivos.**

Se emplea Samba para la compartición de carpetas entre Windows (red interna) y Linux (DMZ), estableciendo un directorio compartido con archivos de pruebas, simulando un entorno corporativo.

4.2.6.5. Implementación de Moloch y Zabbix en red Monitoreo.

El componente Monitoreo cuenta con dos servicios fundamentales, tanto para el estudio interno de los componentes analizados «Zabbix», como para la realización de sniffing en las redes objetivos «Moloch». Moloch emplea «ElasticSearch» como motor de búsqueda, su implementación está expuesta en profundidad en **Anexo *16***, ***Ilustración 37*** muestra el acceso vía web mediante la dirección IP del servidor al puerto «8005». El servidor Zabbix emplea base de datos «MariaDB» y servidor web apache, su implementación y configuración está disponible en ***Anexo 17***, mientras, **Anexo *18*** y **Anexo *19*** detallan la instalación y configuración de los agentes Zabbix en componentes Intranet y DMZ respectivamente, zabbix es accedido vía web mediante: *'http:192.168.1.39/zabbix'*.

Ilustración 37: Web GUI de Moloch



Fuente: La Investigación
Elaborado por: Autor

4.3. Resultados obtenidos en la ETAPA TRES: Identificación de muestras.

4.3.1. Introducción.

Los sistemas informáticos se encuentran diariamente amenazados por software maliciosos con posibilidades de causar pérdidas y cuantiosos daños a organizaciones y empresas, por ello, los investigadores de seguridad a nivel mundial disponen de distintas fuentes de malware con fines educativos, investigativos o desarrollo de herramientas para contrarrestar

amenazas, estas fuentes suelen poseer grandes cantidades de código malicioso con enfoque masivo, como «Hybrid-Analysis», mientras, se encuentra disponibles herramientas de generación de software con fines legítimos y enfocado al control remoto de sistemas, pero, con capacidades de uso indebido y creación de malware dirigido.

4.3.2. Fuentes de muestras consultadas.

Un código malicioso puede obtenerse de diversos medios de acuerdo a su forma de propagación y al sistema que vulnere (Internet, correos electrónicos, dispositivos usb, etc), no obstante, existen organizaciones y sitios web encargados de recopilación y análisis de especímenes sospechosos, si bien, las descargas son restringidas con fines de protección, en muchos casos se necesita de verificación manual por parte de la entidad, justificando los fines del requerimiento o la institución patrocinadora de la investigación. En ***Tabla 15***, se muestras fuentes usuales de malwares consultadas con una breve reseña.

Tabla 15: Base de datos de malware para investigación

Fuente	Descripción	Última Actualización
Contagiodump[46]	Blog de recopilación de malwares categorizado bajo diferentes consideraciones (Tipo de malware, vulnerabilidad afectada, origen)	20/03/2018
Dasmalwerk[47]	Recopila malwares de diversas fuentes en internet.	16/04/2018
hybrid-analysis[48]	Herramienta gratuita de análisis híbrido automatizado de malware mediante Falcon Sandbox, permite subir muestras, analizarlas y compartirlas bajo suscripción, la cual es gratuita para investigadores y académicos pero requiere de evaluación manual del perfil previo a la aceptación.	Actualizado

[46] http://contagiodump.blogspot.com/
[47] http://dasmalwerk.eu/
[48] https://www.hybrid-analysis.com/

kernelmode[49]	Comunidad para discusión y peticiones de muestras de malwares con fines investigativos y académicos, requiere de invitación	Actualizado
malshare[50]	Repositorio de colección de malware para investigadores y resultados YARA (herramienta para clasificar e identificar muestras)	Actualizado
avcaesar[51]	Motor de búsqueda y análisis de muestras de malware a través de varios antivirus	Actualizado
objective-see[52]	Base de datos para malware y adware con afectaciones a dispositivos Mac	No Actualizado
virusign[53]	Repositorio de acceso restringido a muestras de malwares para el mejoramiento de softwares antivirus e investigación	Actualizado
virustotal[54]	Servicio gratuito de análisis de archivos y URLs sospechosos.	Actualizado

Fuente: La Investigación
Elaborado por: Autor

4.3.3. Elección de muestra.

"*Los malware pueden clasificarse según el enfoque del atacante respecto a la masificación de su código malicioso y el objetivo del mismo*" [23]. Este proyecto considera tanto «el enfoque masivo» análogo al marketing masivo o de la escopeta, y el «malware dirigido» diseñado específicamente para atacar no más que la red de una organización, conociendo vulnerabilidades propias de la misma.

El componente Intranet posee características de software masivo, tanto con uso doméstico como empresariales, esto lo hace propenso a infecciones de malware; mientras, el componente DMZ, representando servicios empresariales, puede ser claro objetivo de malware dirigido. En ***Tabla 16***, se resume el enfoque y características usado para elección de muestras a estudiar.

[49] http://www.kernelmode.info/forum/viewforum.php?f=16
[50] https://malshare.com/
[51] https://avcaesar.malware.lu/
[52] objective-see
[53] http://www.virusign.com/
[54] https://www.virustotal.com/en/

Tabla 16: Enfoque y características de muestras

Componente	*Enfoque*	*Características*
Intranet	Masivo	• Primer espécimen hallado a una fecha relativamente reciente al desarrollo del proyecto. • Posibilidad de ejecución en equipos de 32 bits. • Comportamiento sospechoso en la red. • Características de spyware, backdoor o worm.
DMZ	Dirigido	• Creado según particularidades del servidor DMZ. • Características de RAT[55] o APT[56]. • Uso de encriptación en el transporte. • Posibilidad de realizar robo de información u obtención de credenciales.

Fuente: La Investigación
Elaborado por: Autor

4.3.4. Espécimen para componente Intranet.

Mediante indagación de distintas bases de datos y obtención de los permisos correspondientes para la descarga de muestras de estudio, se opta por la utilización de Hybrid-Analysis como fuente, siendo un servicio gratuito de análisis dinámico automático, posibilita la compartición de la muestra subida con una gran comunidad de investigadores; la obtención de permisos necesarios para descarga, sigue una estricta petición con corroboración manual, tardando veinte y cuatro horas su aceptación, mediante la explicación de los fines de la muestras, objetivos del proyecto y contar con un correo institucional validado por la Universidad Técnica Estatal de Quevedo. Siguiendo las características establecidas con anterioridad en ***Tabla 15***, se eligió al espécimen "wayne.exe"[57], muestra

[55] Remote Access Tool

[56] Advanced persistent threat

[57] https://www.hybrid-analysis.com/sample/dbdb13156ea0cf09bb1daccaaf42ee2b29b286bc4ca282c7ae686b4b05ffa157?environmentId=100

estudiada a profundidad en vmray.com[58] (***Ilustración 38***) y de origen establecido en ***Ilustración 39*** como generado por «Agent Tesla»[59], analizado por Hybrid-Analysis el 8 de septiembre de 2018 (ver ***Ilustración 40***) y expuesto por primera vez por VirusTotal el 3 de septiembre de 2018 (ver ***Ilustración 41***).

Ilustración 38: Calificación obtenido por VMRAY

Fuente: vmray.com
Elaborado por: Autor

Ilustración 39: Origen de muestra "wayne.exe"

Fuente: vmray.com
Elaborado por: Autor

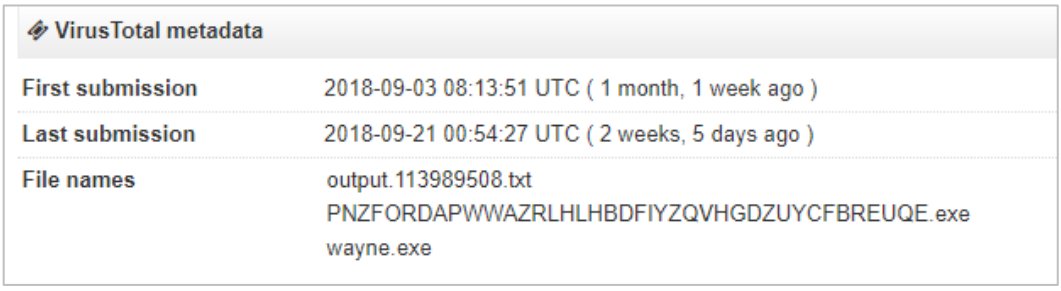
Ilustración 40: Espécimen propuesto para análisis en componente Intranet

Fuente: Hybrid-Analysis
Elaborado por: Autor

[58] https://www.vmray.com/analyses/dbdb13156ea0/report/overview.html

[59] Potente y moderno registrador de pulsaciones

Ilustración 41: Primera aparición de muestra por VirusTotal



Fuente: VirusTotal.com
Elaborado por: Autor

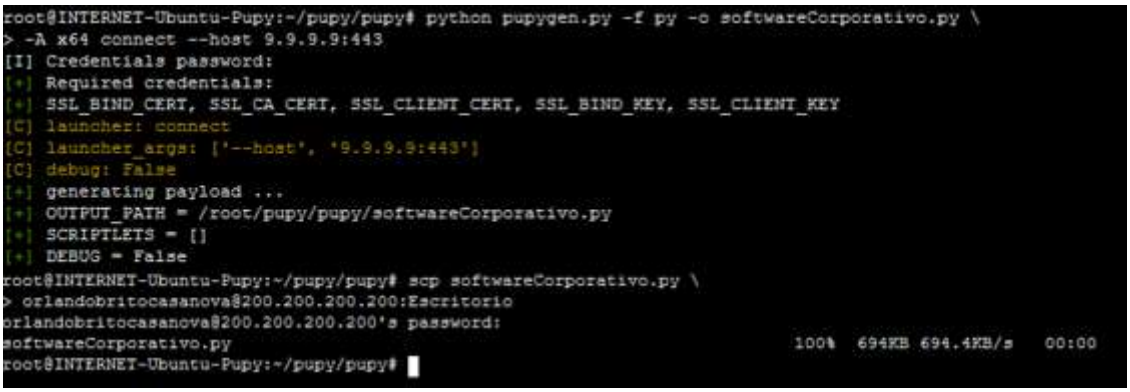
4.3.5. Espécimen para componente DMZ.

Un malware objetivo está enfocado en características específicas de la red o sistema a comprometer. Sus creadores comunes son investigadores de seguridad, hacktivista, ciber-delincuentes y ciber-terroristas, usualmente poseen grandes habilidades de programación, así como vastos conocimientos de los sistemas a vulnerar. No obstante, existen herramientas disponibles para generación de software con capacidades maliciosas, aunque los fines propuestos por los desarrolladores se alejan de usos malignos, concentrándose en la investigación, educación y en herramientas legítimas de control de acceso remoto (RAT), pueden y son usados para obtención de malware. Estas herramientas son completamente legales en muchos países del mundo, ya que sus leyes prohíben la distribución y explotación de código malicioso, más no su creación o generación.

Pupy es un proyecto creado y desarrollado en github por el usuario n1nj4sec, descrito como herramienta de acceso remoto y post-explotación. Esta contribución posee fines educativos y de investigación, debido a la gratuidad de su descarga e instalación, no posee impedimento alguno para ser usados con un propósito distinto y poco ético. Tiene capacidades multiplataforma, pudiendo generar cargas para diferentes plataformas (Windows, Linux, OSX, Android).

En ***Ilustración 42*** se presenta el proceso para creación de malware "softwareCorporativo.py" con características propias del sistema a vulnerar, como: escrito en python, arquitectura de 64 bits y conexión saliente mediante el puerto 443, permitido en el firewall de la zona DMZ. También se muestra el mecanismo usado para el transporte hacia el sistema objetivo.

Ilustración 42: Creación de espécimen "softwareCorporativo.py" para estudio en componente DMZ



Fuente: La investigación
Elaborado por: Autor

4.4. Resultados obtenidos en la ETAPA CUATRO: Análisis dinámico de malware.

4.4.1. Introducción.

El análisis dinámico de malware es crucial para conocer las capacidades, comportamiento y objetivos de software sospechosos, donde un laboratorio aislado de análisis posee un papel importante para el desarrollo de una correcta investigación; por ello es necesario una adecuada configuración de las herramientas empleadas, conocimiento del estado previo de la red o sistema, análisis automático (escaneo e indagación de muestra) mediante herramientas gratuitas en línea y las debidas precauciones durante la ejecución del espécimen.

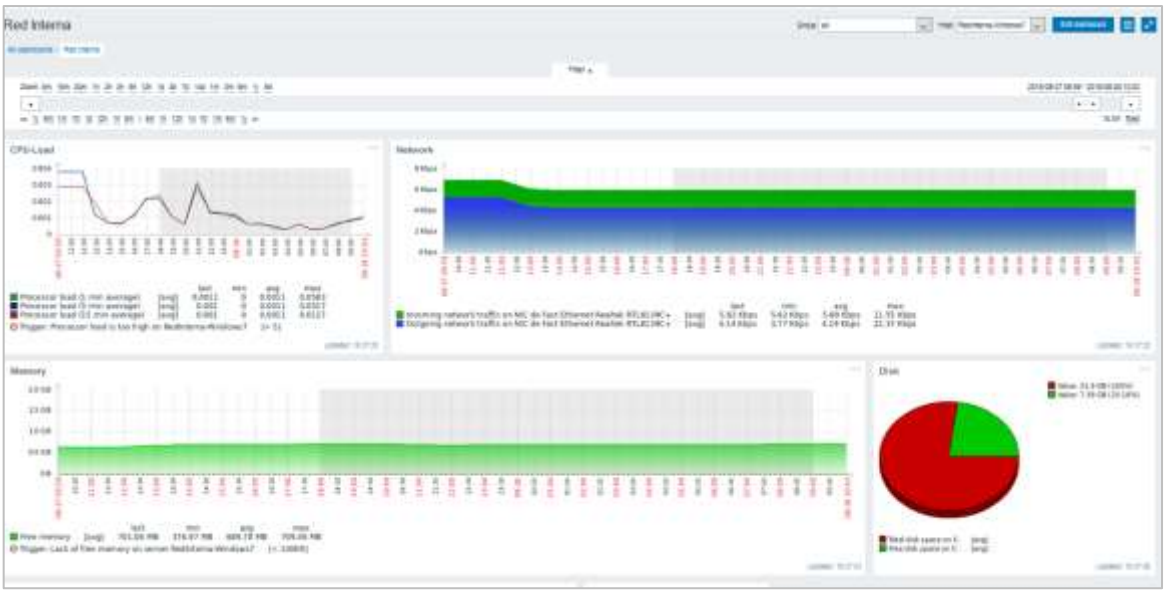
4.4.2. Análisis de estado previo del sistema en conjunto.

El analizar la red, en su estado de pre-infección permite la obtención del comportamiento normal de los sistemas y un punto de partida en comparaciones posteriores con ejecución del malware. Se estudia el comportamiento y rendimiento de la red y sistemas tanto con simulación de Internet (INetSIM) como con salida al mundo exterior una vez se haya tomado las debidas precauiciones.

4.4.2.1. Análisis previo de red con implementación de INetSIM.

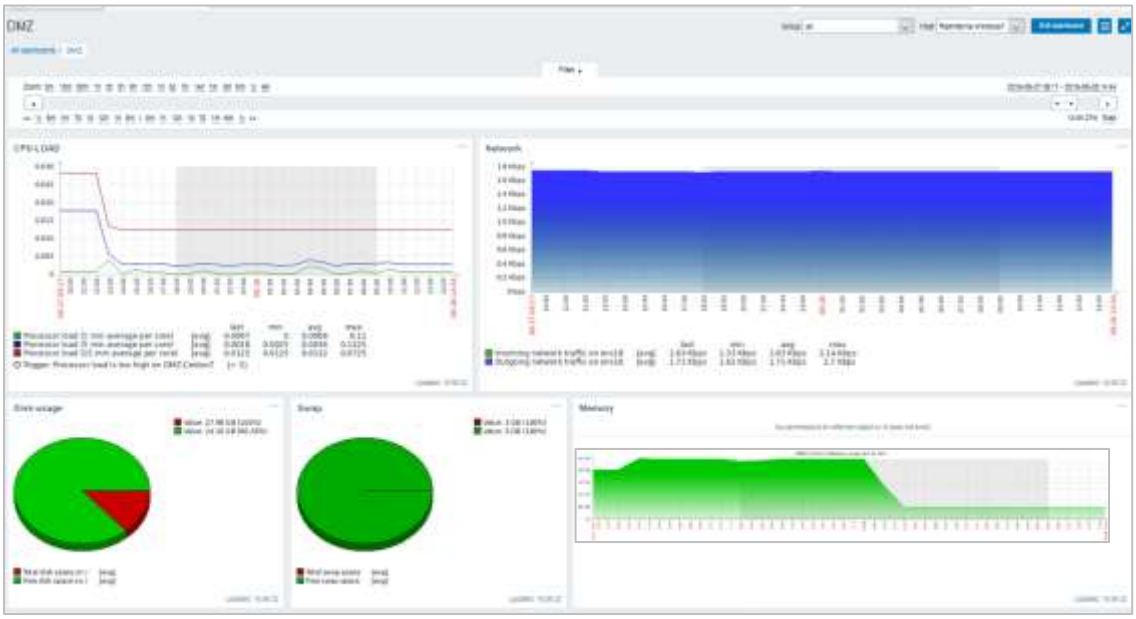
La medición se realizó en un periodo de veinticuatro horas, entre las 10:00 AM del 27/08/18 y 10:00 AM del 28/08/17. En ***Ilustración 43*** e ***Ilustración 44***, muestra las gráficas de rendimiento obtenidas por zabbix para los componentes Intranet y DMZ respectivamente.

Ilustración 43: Rendimiento de componente Intranet



Fuente: La Investigación
Elaborado por: Autor

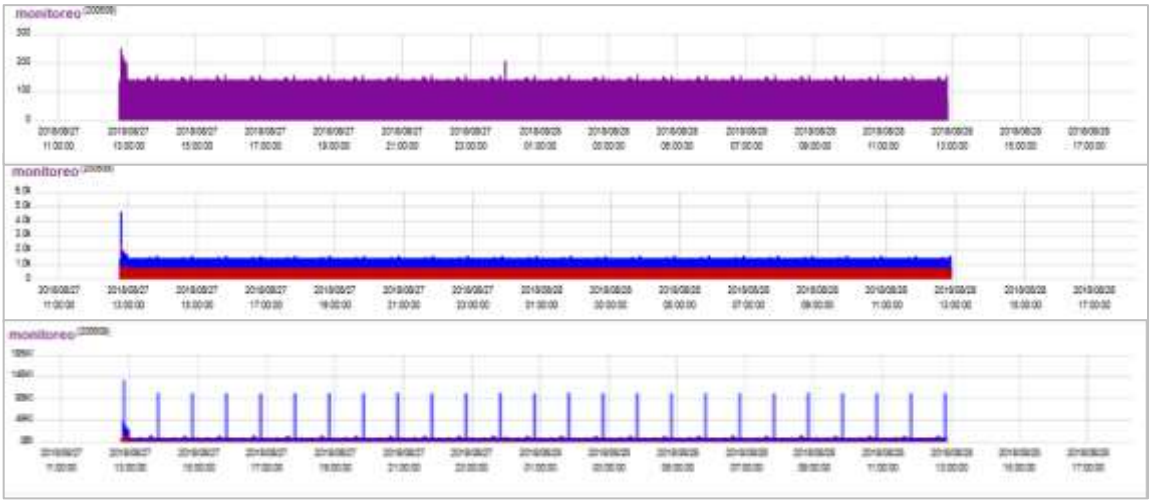
Ilustración 44: Rendimiento del componente DMZ



Fuente: La Investigación
Elaborado por: Autor

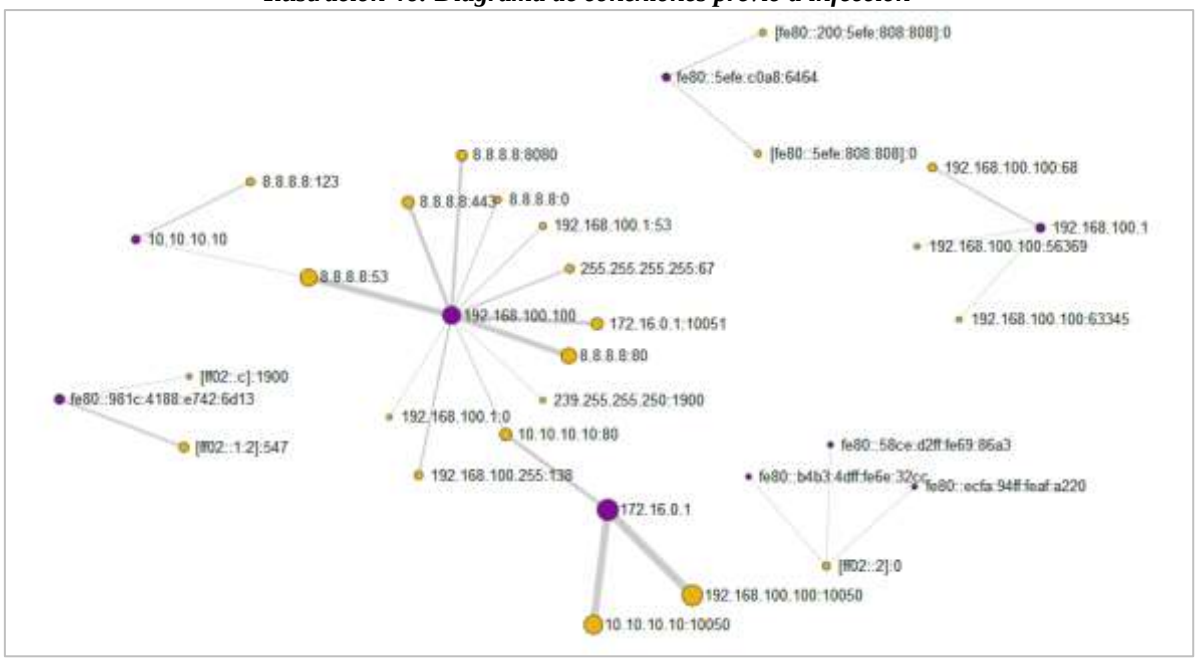
El estudio de los paquetes cursados por las redes objetivos (vmbr100 → Intranet y vmbr200 → DMZ) se realiza empleando la herramienta de escucha de paquete «Moloch» con base de datos Elasticsearch, en conjunto con el demonio «daemonlogger» ejecutado en el host hipervisor proxmox para realizar un "espejado" de paquetes cursados en las redes antes mencionadas a la red vmbr600. El proceso de sniffear de redes se específica en **Anexo *20***. En ***Ilustración 45***, muestra gráficas del uso de la red según sesiones, paquetes y data bytes cursados, mientras, **Ilustración 46** muestra el diagrama de conexiones del sistema completo e ***Ilustración 47*** las conexiones específicas e independientes de los componentes Intranet.

Ilustración 45: Gráficas del uso de la red por Moloch según sesiones, paquetes y databytes



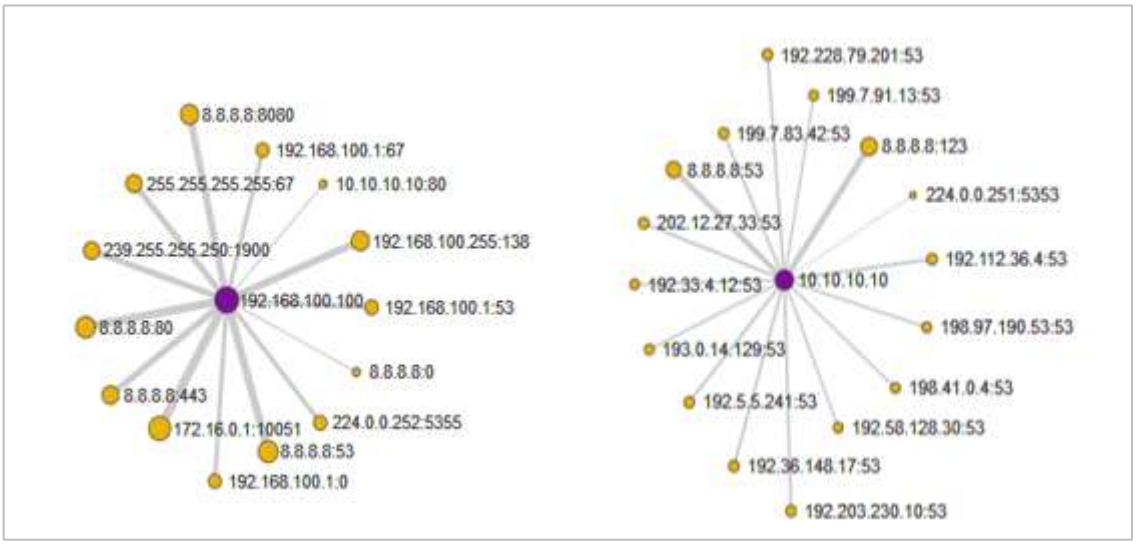
Fuente: La Investigación
Elaborado por: Autor

Ilustración 46: Diagrama de conexiones previo a infección



Fuente: La Investigación
Elaborado por: Autor

Ilustración 47: Diagrama de conexiones de componente Intranet y DMZ



Fuente: La Investigación
Elaborado por: Autor

INetSIM brinda la emulación de varios protocolos comunes de red, en su mayoría intenta devolver un resultado ante cualquier petición, permitiendo el desarrollo y mejor ejecución del malware y el estudio de su funcionamiento. Las peticiones realizadas se verifican en el archivo ***'/var/log/inetsim/service.log'***. ***Ilustración 48*** muestra la clasificación de los logs según fechas y el tamaño, e ***Ilustración 49*** denota el formato de los paquetes guardados; Los registros se obtuvieron desde el día 27-08-2018 desde las 17:18 UTC.

Ilustración 48: Logs de análisis previo obtenido de INetSIM

```
root@INTERNET-Ubuntu:/var/log/inetsim# cat  service.log |grep 2018-08-27 > 2018-08-27_Previo.log
root@INTERNET-Ubuntu:/var/log/inetsim# cat  service.log |grep 2018-08-28 > 2018-08-28_Previo.log
root@INTERNET-Ubuntu:/var/log/inetsim# cat 2018-08-27_Previo.log |wc -l
12547
root@INTERNET-Ubuntu:/var/log/inetsim# cat 2018-08-28_Previo.log |wc -l
14433
root@INTERNET-Ubuntu:/var/log/inetsim# ll -h 2018-08-28_Previo.log 2018-08-27_Previo.log
-rw-r--r-- 1 root root 1.2M Sep 12 12:53 2018-08-27_Previo.log
-rw-r--r-- 1 root root 1.4M Sep 12 12:53 2018-08-28_Previo.log
root@INTERNET-Ubuntu:/var/log/inetsim#
```

Fuente: La Investigación
Elaborado por: Autor

Ilustración 49: Peticiones obtenidas por servidor INetSIM durante análisis previo infección

```
  GNU nano 2.2.6                File: 2018-08-27_Previo.log

[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] connect
[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] recv: VN = 4,  Mode = 3,  LI = 3
[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] recv: Stratum = 0,  Poll = 6,  Precisio
[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] recv: Root Delay = 0,  Root Dispersion
[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] recv: Reference Identifier = INIT
[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] recv: Reference Timestamp =    0.00000
[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] recv: Originate Timestamp =    0.00000
[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] recv: Receive Timestamp =    0.00000
[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] recv: Transmit Timestamp = 1535390284.7
[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] send: VN = 4,  Mode = 4,  LI = 0
[2018-08-27 17:18:05] [1801] [ntp_123_udp 2110] [8.8.8.1:123] send: Stratum = 2,  Poll = 6,  Precisio
```

Fuente: La Investigación
Elaborado por: Autor

4.4.2.2. Análisis previo de red con salida a Internet.

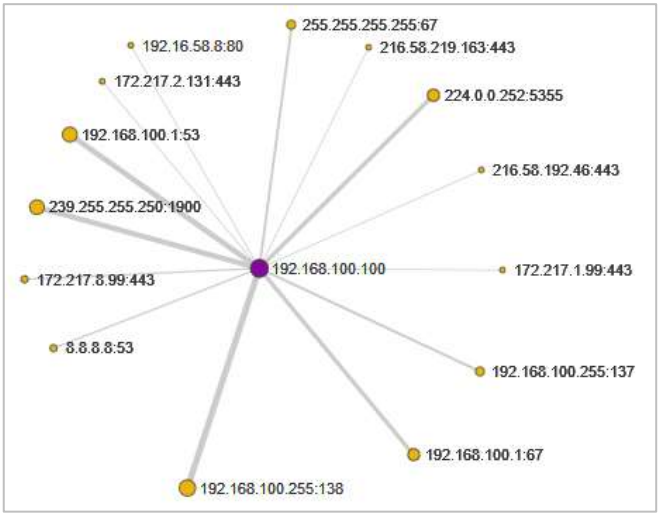
El análisis se enfoca en el comportamiento del componente Intranet, al estar expuesto a malware desconocido y foráneo, contrario al componente DMZ donde sus conexiones se encuentran establecidas. ***Ilustración 50*** expone el inicio del servicio «molochcapture» usado para la escucha de paquete en componente Monitoreo; ***Ilustración 51*** presenta las conexiones establecidas por componente Intranet.

Ilustración 50: Inicio de servicio molochcapture en componente Monitoreo

```
root@monitoreo:~# systemctl status molochcapture
* molochcapture.service - Moloch Capture
   Loaded: loaded (/etc/systemd/system/molochcapture.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2018-10-05 22:10:28 UTC; 6s ago
  Process: 2182 ExecStartPre=/data/moloch-nightly/bin/moloch_config_interfaces.sh (code=exited, status=
 Main PID: 2192 (sh)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/molochcapture.service
           |-2192 /bin/sh -c /data/moloch-nightly/bin/moloch-capture -c /data/moloch-nightly/etc/confi
           `-2193 /data/moloch-nightly/bin/moloch-capture -c /data/moloch-nightly/etc/config.ini

Oct 05 22:10:28 monitoreo systemd[1]: Starting Moloch Capture...
Oct 05 22:10:28 monitoreo systemd[1]: Started Moloch Capture.
```

Fuente: La Investigación
Elaborado por: Autor

Ilustración 51: Conexiones establecidas durante análisis previo con salida a Internet



Fuente: La Investigación
Elaborado por: Autor

4.4.3. Análisis automático online de especímenes a estudiar.

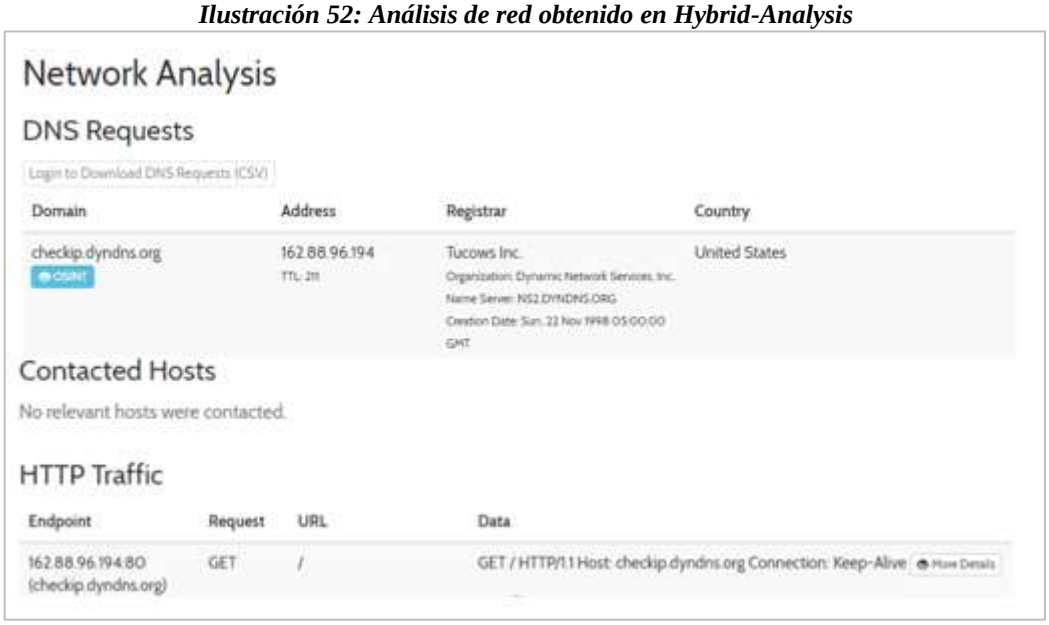
El análisis automático es una pieza crucial en la realización de análisis de malware, muestra resultados anteriores, compatibilidad con muestras conocidas, estudio de alcance y demás características. Los especímenes establecidos en la etapa dos del presente proyecto, son analizados mediante diversas herramientas, como sandbox online (Hybrid-Analysis) y servicios de multi-escáneres (VirusTotal, Spyral Scanner).

4.4.3.1. Análisis automático de muestra masivo "wayne.exe" mediante Hybrid-Analysis.

Hybrid-Analysis es un *"servicio gratuito de análisis de malware para la comunidad que detecta y analiza amenazas desconocidas utilizando una tecnología de única de análisis híbrido"* [49]. Por las características presentadas del malware de estudio, se emplea un entorno "Windows 7 64 bit" (ver **Anexo *21***), obteniendo valoración de malicioso (ver **Anexo *22***) e indicativos de: Adware, autorun, backdoor, crypt, dialer, downloader, exploit, keylogger, ransomware, riskware, rootkit, toolbar y worm.

El reporte generado por "Falcon Sandbox" se halla almacenado en *«https://www.hybrid-analysis.com/sample/dbdb13156ea0cf09bb1daccaaf42ee2b29b286bc4ca282c7ae686b4b05ffa157/5b930bb17ca3e152a6718c23"*», mientras, ***Ilustración 52*** presenta el comportamiento de red anómalo del análisis de la muestra indicada.

Ilustración 52: Análisis de red obtenido en Hybrid-Analysis



Fuente: Hybrid-Analysis.com
Elaborado por: Autor

4.4.3.2. Escaneo de malware masivo "wayne.exe" mediante VirusTotal.

VirusTotal es un multi-escaner gratuito de malware creado por Hispasec Sistemas en 2004 y adquirido por Google Inc en 2012. Emplea una gran variedad de antivirus para escanear con mayor efectividad archivos y URLs sospechosos. El espécimen "wayne.exe" posee un ratio de detección de 46/67, indicativo de amenaza potencialmente peligrosa. En ***Tabla 17***, se expone los resultados de antivirus populares (resultados completos en **Anexo *23***).

Tabla 17: Extracto de escaneo por VirusTotal

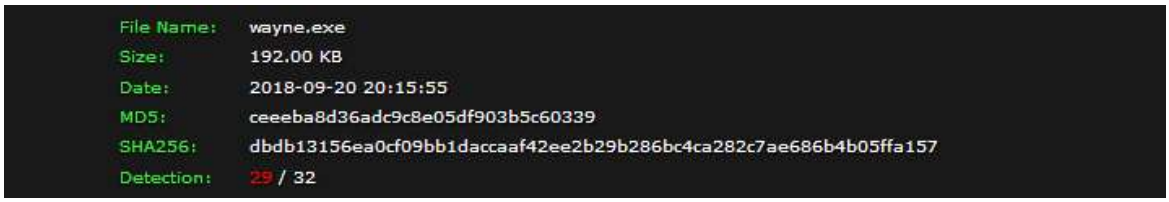
Antivirus	Resultado
Avast	MSIL:Crypt-AAL [Trj]
AVG	MSIL:Crypt-AAL [Trj]
BitDefender	Gen:Variant.Razy.182576
ClamAV	Win.Dropper.Razy-6519812-0
ESET-NOD32	a variant of MSIL/Spy.Agent.AES
Kaspersky	HEUR:Trojan.MSIL.Generic
Malwarebytes	Trojan.PasswordStealer.MSIL
McAfee	Trojan-FPEL!CEEEBA8D36AD
Panda	Trj/GdSda.A
Sophos AV	Mal/Generic-S
TrendMicro	TSPY_NEGASTEAL.SMILA
Fortinet	MSIL/Injector.PE!tr
Ad-Aware	Gen:Variant.Razy.182576
Palo Alto Networks	generic.ml

Fuente: VirusTotal.com
Elaborado por: Autor

4.4.3.3. Escaneo de malware masivo "wayne.exe" mediante Spyral Scanner.

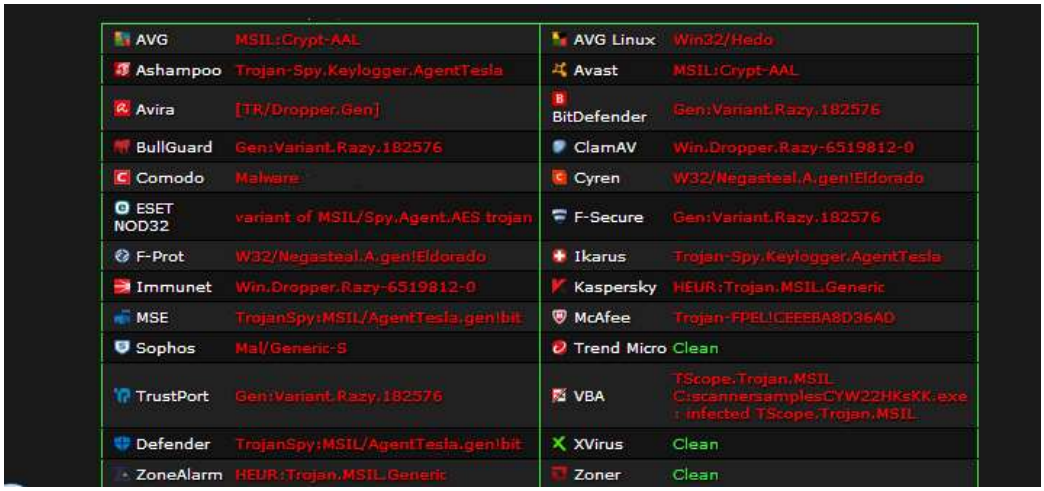
"Solo el 25 por ciento de las muestras pueden ser encontradas en al menos un multi-escáner tradicional, mientras el que restante 75 por ciento nunca será visto" [50], esa es la importancia del empleo de escáneres no distribuidos, como Spyral-Scanner. ***Ilustración 53*** expone el resultado general del análisis automático realizado, mientras ***Ilustración 54***.

Ilustración 53: Resultado general de análisis mediante SpyralScanner de muestra «wayne.exe»



Fuente: Spyral Scanner
Elaborado por: Autor

Ilustración 54: Escaneo de espécimen "wayne.exe" empleando Spyral Scanner



AVG	MSIL:Crypt-AAL	AVG Linux	Win32/Hedo
Ashampoo	Trojan-Spy.Keylogger.AgentTesla	Avast	MSIL:Crypt-AAL
Avira	[TR/Dropper.Gen]	BitDefender	Gen:Variant.Razy.182576
BullGuard	Gen:Variant.Razy.182576	ClamAV	Win.Dropper.Razy-6519812-0
Comodo	Malware	Cyren	W32/Negasteal.A.gen!Eldorado
ESET NOD32	variant of MSIL/Spy.Agent.AES trojan	F-Secure	Gen:Variant.Razy.182576
F-Prot	W32/Negasteal.A.gen!Eldorado	Ikarus	Trojan-Spy.Keylogger.AgentTesla
Immunet	Win.Dropper.Razy-6519812-0	Kaspersky	HEUR:Trojan.MSIL.Generic
MSE	TrojanSpy:MSIL/AgentTesla.gen!bit	McAfee	Trojan-FPEL!CEEEBA8D36AD
Sophos	Mal/Generic-S	Trend Micro	Clean
TrustPort	Gen:Variant.Razy.182576	VBA	TScope.Trojan.MSIL C:\scanner\samples\CYW22HKsKK.exe : infected TScope.Trojan.MSIL
Defender	TrojanSpy:MSIL/AgentTesla.gen!bit	XVirus	Clean
ZoneAlarm	HEUR:Trojan.MSIL.Generic	Zoner	Clean

Fuente: Spyral Scanner
Elaborado por: Autor

4.4.3.4. Análisis automático de malware dirigido “softwareCorporativo.py” mediante Hybrid-Analysis.

Al ser un espécimen creado para desenvolverse en ambientes Linux primordialmente, se establece al mismo como entorno de análisis automático usando las tecnología híbridas de Hybrid-Analysis (ver **Anexo *24***). ***Ilustración 55*** presenta la clasificación de no amenaza según el análisis realizado[60]. No obstante, existe errores en el transcurso de la ejecución de Falcon Sandbox, impidiendo la obtención de un reporte (ver **Anexo *25***).

Ilustración 55: Análisis automático de muestra "softwareCorporativo.py" en Hybrid-Analysis

Fuente: Hybrid-Analysis
Elaborado por: Autor

[60] https://www.hybrid-analysis.com/sample/892587a308979c4335e6d3d1ec78a4f6c3828d511f639511f5d848590f6b6f63

4.4.3.5. Escaneo de malware dirigido "softwareCorporativo.py" mediante VirusTotal.

La muestra de estudio obtuvo un ratio de detección equivalente a 1/56 (ver ***Ilustración 56***), siendo detectada únicamente por antivirus DrWeb como "Python.Siggen.5" y, no detectado o imposibilitado de análisis por los antivirus restantes (Ver **Anexo *26***)

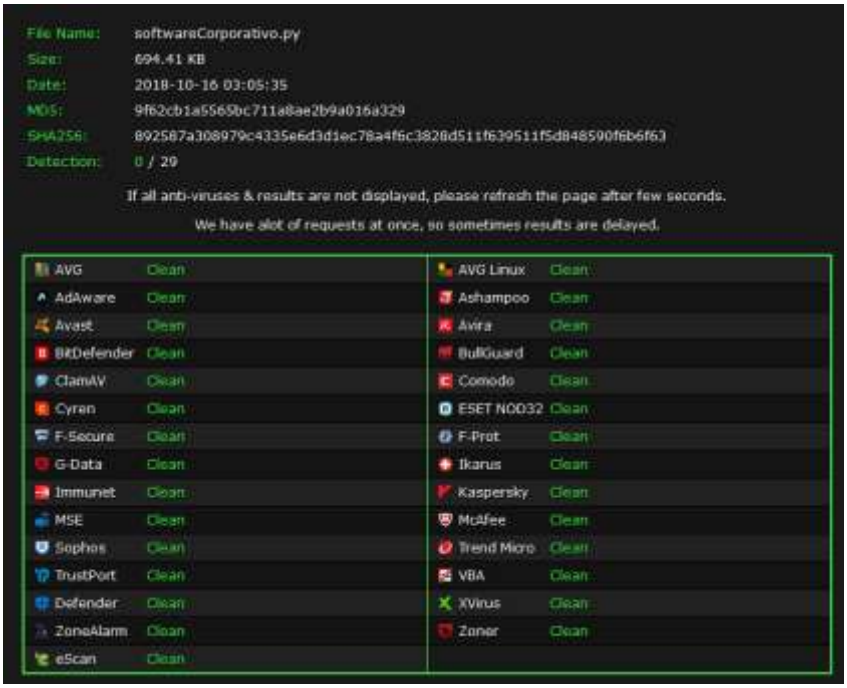
Ilustración 56: Escaneo de muestra "softwareCorporativo.py" mediante VirusTotal

Fuente: VirusTotal.com
Elaborado por: Autor

4.4.3.6. Escaneo de malware dirigido "softwareCorporativo.py" mediante Spyral Scanner.

El archivo escaneado presenta cero detecciones entre los diferentes antivirus empleados, siendo establecido como fichero no peligroso (Ver **Ilustración 57**).

Ilustración 57: Escaneo de muestra "softwareCorporativo.py" mediante Spyral Scanner



Fuente: Spyral Scanner
Elaborado por: Autor

4.4.4. Análisis dinámico de muestra “wayne.exe” ejecutada en componente Intranet.

La ejecución del espécimen se realiza en dos topologías ya diferenciadas según su salida a Internet (real o simulación). Es importante desactivar firewall de Windows y bit defender en la máquina objetivo y brindar un ambiente propicio para el estudio de la totalidad de cualidades de la muestra.

4.4.4.1. Análisis dinámico empleando INetSIM.

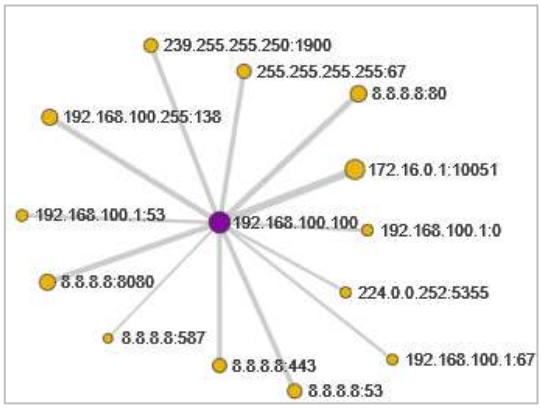
La muestra de estudio se ejecutó a las 13:28 y 20:40 hasta las 21:48 (GMT-5) en el transcurso del día 21 de Septiembre del 2018, careciendo de comportamiento visible o drástico, esto puede ser indicativo de errores de ejecución por archivos recibidos de INetSIM que no cumplen las necesidades esperadas por el espécimen. ***Ilustración 58*** evidencia el rendimiento del componente Intranet durante le ejecución del software.

Ilustración 58: Rendimiento de componente Intranet durante ejecución de "wayne.exe"

Fuente: La Investigación
Elaborado por: Autor

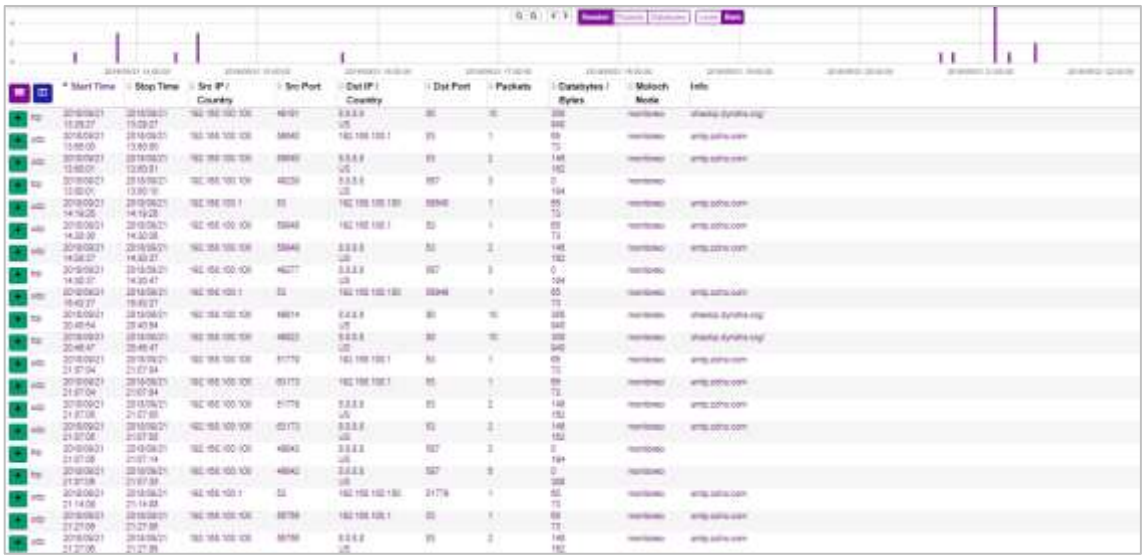
Ilustración 59 exhibe las conexiones realizadas por la componente Intranet durante el periodo de evaluación. El carecimiento de direcciones IP diferentes corresponde al funcionamiento de INetSim, cual resuelve cada petición DNS con su propia IP. Sin embargo, existen conexiones inusuales al puerto 587 correspondiente al puerto «submission» del protocolo SMTP, pudiendo ser empleado en el envío de correo spam. ***Ilustración 60*** muestra los paquetes capturados por Moloch e ***Ilustración 61*** indica el contenido (vacío) de paquete con dirección puerto destino 587.

Ilustración 59: Conexiones establecidas por componente Intranet durante ejecución de "wayne.exe"



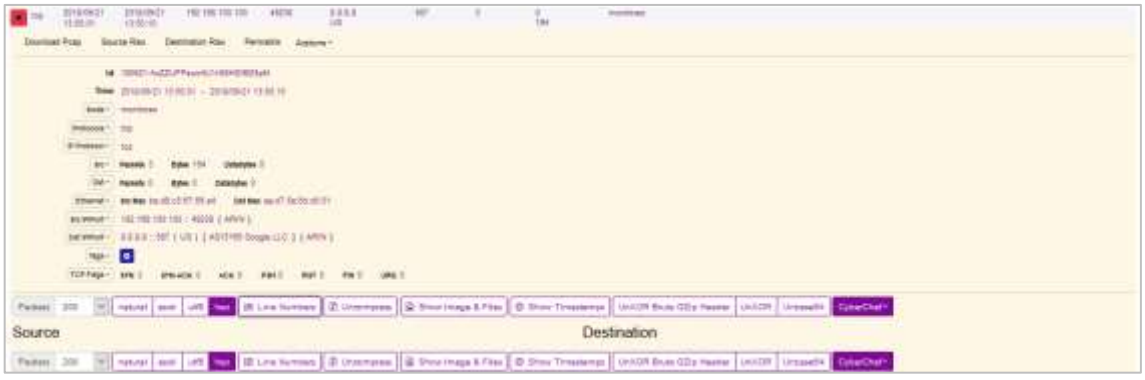
Fuente: La Investigación
Elaborado por: Autor

Ilustración 60: Paquetes obtenidos durante análisis de "wayne.exe" mediante Moloch



Fuente: La Investigación
Elaborado por: Autor

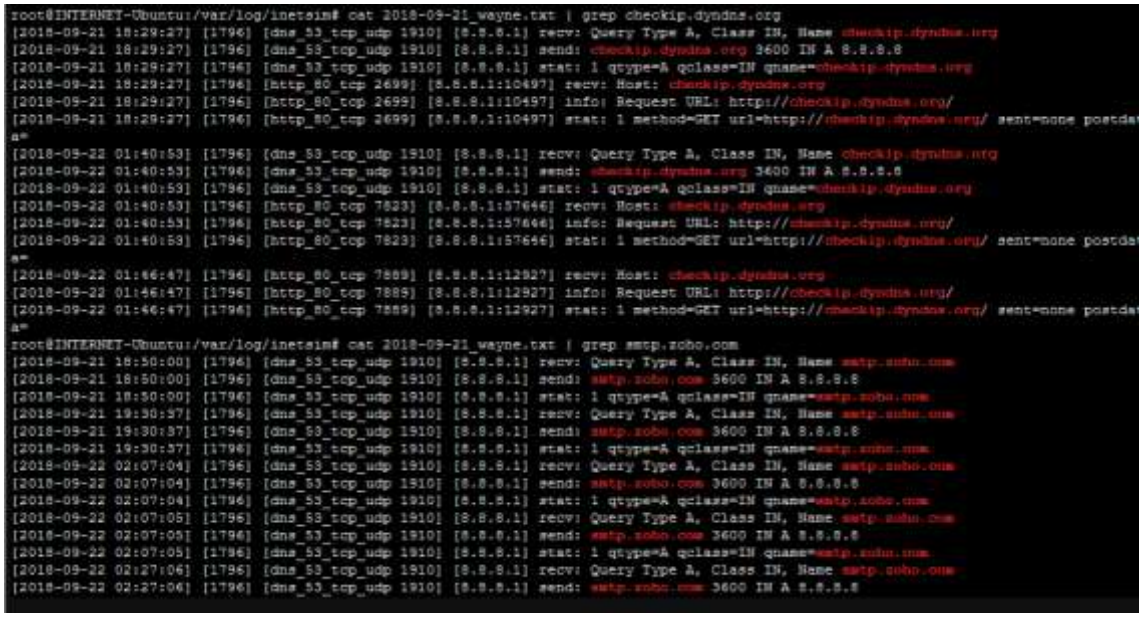
Ilustración 61: Paquete sospechoso con puerto destino 587



Fuente: La Investigación
Elaborado por: Autor

Con los indicios establecidos en los registros de paquetes obtenidos por Moloch, se indaga en las peticiones realizadas hacia el servidor de simulación de Internet. Es preferible el aislamiento de los logs según la fecha estudiada, para tener mayor rapidez de consulta (Ver **Anexo** ***27***). ***Ilustración 62*** presenta las peticiones y repuesta del servicio INetSim a requerimientos producidos por muestra "wayne.exe". No existe registro alguno de interacción con el puerto 587 en '/var/log/inetsim/service.log'.

Ilustración 62: Peticiones y respuesta de INetSim a requerimientos de "wayne.exe"

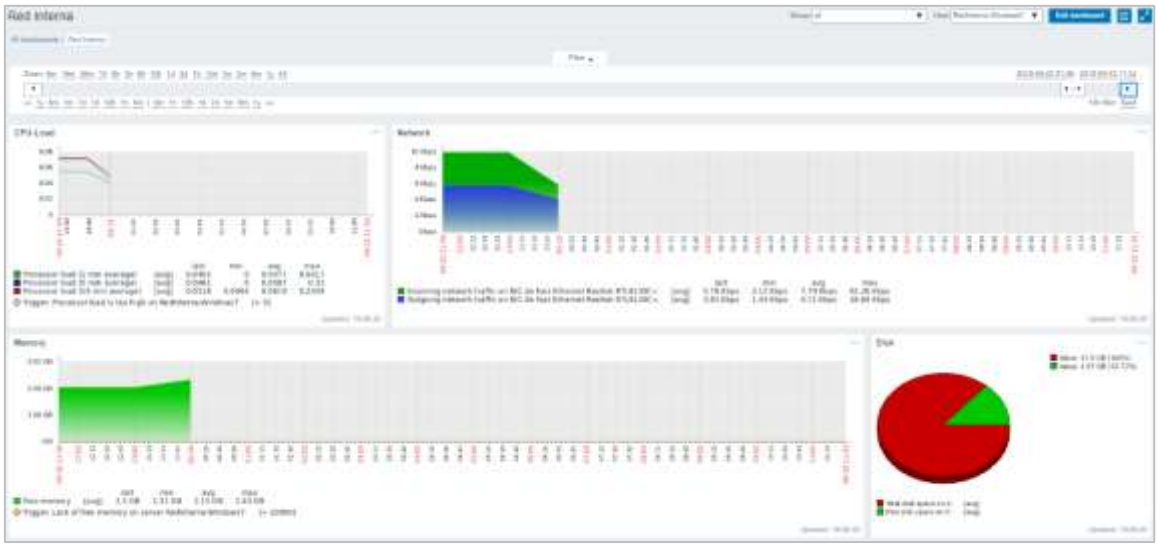


Fuente: La Investigación
Elaborado por: Autor

4.4.4.2. Análisis dinámico con salida real a Internet.

Los intentos de conexión con servidores DNS y SMTP externos son evidencias de comportamientos anómalos característicos de spyware, downloader y gusanos informáticos, pero no se obtuvo información de relevancia, cabe la posibilidad de que el funcionamiento de la muestra se encuentra truncada por no recibir las respuestas esperadas, por ello es justificable la realización de análisis dinámico con salida real a internet. La muestra es ejecutada en el transcurso de tiempo (desde 22/09/18 23:50:00, hasta 23/09/18 16:42:00). ***Ilustración 63*** muestra el rendimiento del componente Intranet, es de notar cómo el servicio «zabbix» dejó de recibir respuestas del host (192.168.100.100) debido al cambio de dirección IP (192.168.100.102) denotado en ***Ilustración 64***.

Ilustración 63: Rendimiento de componente Intranet durante ejecución de "wayne.exe" con salida real a Internet



Fuente: La Investigación
Elaborado por: Autor

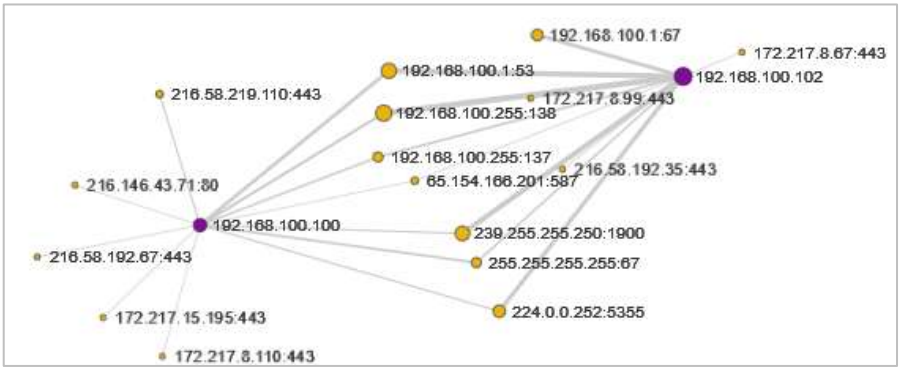
Ilustración 64: Cambio de dirección IP en componente Intranet

+	icmp	2018/09/23 00:37:04	2018/09/23 00:37:04	192.168.100.1	0	192.168.100.100	0	2	0 124	monitoreo
+	udp	2018/09/23 00:37:04	2018/09/23 00:37:15	192.168.100.100	68	255.255.255.255	67	4	1,360 1,392	monitoreo
+	udp	2018/09/23 00:37:09	2018/09/23 00:37:15	192.168.100.1	67	192.168.100.102	68	3	1,002 1,026	monitoreo
+	icmp	2018/09/23 00:37:15	2018/09/23 00:37:15	192.168.100.1	0	192.168.100.102	0	2	0 124	monitoreo
+	icmp6	2018/09/23 00:37:15	2018/09/23 00:37:19	fe80::981c:4188:e74 2:6d13	0	ff02::16	0	11	0 1,010	monitoreo
+	udp	2018/09/23 00:37:16	2018/09/23 00:37:37	192.168.100.102	137	192.168.100.255	137	24	2,448 2,640	monitoreo

Fuente: La Investigación
Elaborado por: Autor

Ilustración 65 presenta las conexiones realizadas por el componente Intranet con salida real a Intranet, obteniendo nuevas direcciones a estudiar y denotando el cambio de IP; Los intentos de conexión se encuentran expresando en ***Ilustración 66*** (petición DNS y HTTP) e ***Ilustración 67*** con envío de paquetes al puerto 587 de dirección externa.

Ilustración 65: Conexiones realizadas durante ejecución de "wayne.exe" con salida real a Internet



Fuente: La Investigación
Elaborado por: Autor

Ilustración 66: Peticiones realizadas por "wayne.exe" con salida real de Internet

Fuente: La Investigación
Elaborado por: Autor

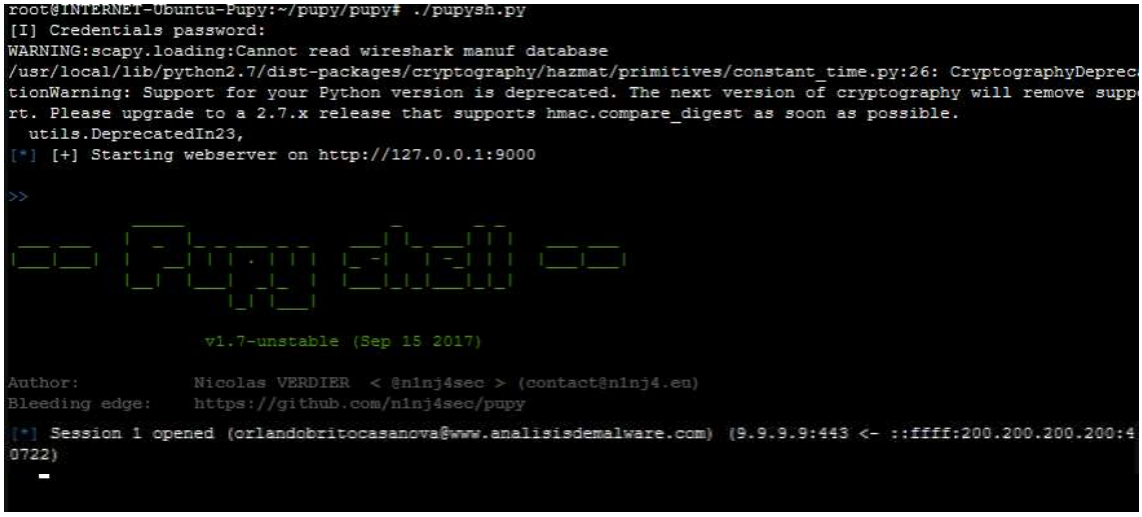
Ilustración 67: Paquete enviado a puerto 587 de ip externa, con salida real de Internet

Fuente: La Investigación
Elaborado por: Autor

4.4.5. Análisis dinámico de muestra “softwareCorporativo.py” ejecutada en componente DMZ.

Al estar desarrollado empleando el lenguaje de programación python, es posible la ejecución de “softwareCorporativo.py”en varios entornos, incluyendo CentOS, sistema operativo de componente DMZ. El correcto funcionamiento del espécimen requiere de acceso del servidor Pupy a máquina objetivo, obteniéndose mediante las configuraciones de red pertinentes y la habilitación de “ip forwarding” en componente Internet-INetSIM. ***¡Error! o se encuentra el origen de la referencia.*** expone el proceso de levantamiento de servicio y establecimiento de sesión en servidor Pupy. Se realiza una post-explotación sencilla del sistema empleando posibilidades brindadas por RAT Pupy, tal como información de usuario, id de sesión, captura de pantalla, obtención de pulsaciones de teclado, escaneo de puertos, habilitación de persistencia y búsqueda de archivos (ver **Anexo *28***).

Ilustración 68: Levantamiento de servidor Pupy y establecimiento de sesión.

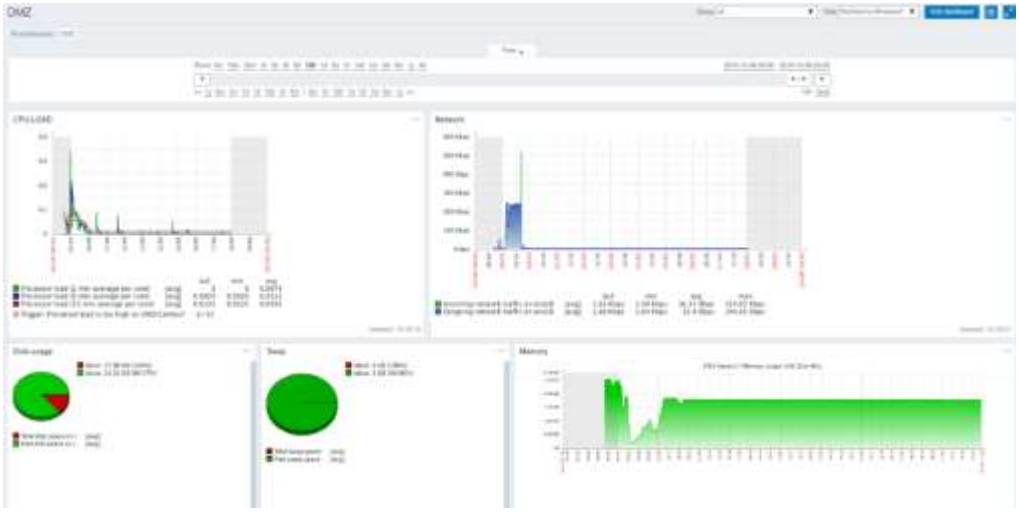


Fuente: La investigación
Elaborado por: Autor

4.4.5.1. Comportamiento de red y rendimiento de componente DMZ, durante ejecución de “softwareCorporativo.py”.

Ilustración 69 revela el rendimiento interno del componente DMZ obtenido mediante el servicio Zabbix, ***Ilustración 70*** manifiestan los paquetes cursados por la red (filtrado por dirección IP destino 9.9.9.9) durante el periodo de evaluación iniciado el 09-10-2018 a las 9:15 am, y culminado en misma fecha a las 20:00 pm, e ***Ilustración 71*** denota el contenido encriptado de un registro.

Ilustración 69: Rendimiento de componente DMZ durante ejecución de "softwareCorporativo.py" mediante Zabbix



Fuente: La investigación
Elaborado por: Autor

Ilustración 70: Paquetes obtenidos por Moloch durante ejecución de "softwareCorporativo.py"

Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info
2018/10/09 09:22:56	2018/10/09 09:34:22	10.10.10.10	49722	9.9.9.9 FR	443	366	47,600 71,376	monitoreo	
2018/10/09 09:22:56	2018/10/09 09:46:39	10.10.10.10	49722	9.9.9.9 FR	443	3,174	3,228,255 3,437,739	monitoreo	
2018/10/09 09:22:56	2018/10/09 10:09:33	10.10.10.10	49722	9.9.9.9 FR	443	4	0 264	monitoreo	
2018/10/09 09:22:56	2018/10/09 10:34:38	10.10.10.10	49722	9.9.9.9 FR	443	6	0 396	monitoreo	
2018/10/09 09:22:56	2018/10/09 10:54:42	10.10.10.10	49722	9.9.9.9 FR	443	4	0 264	monitoreo	
2018/10/09 09:22:56	2018/10/09 11:34:51	10.10.10.10	49722	9.9.9.9 FR	443	6	0 396	monitoreo	
2018/10/09 09:22:56	2018/10/09 11:44:53	10.10.10.10	49722	9.9.9.9 FR	443	4	0 264	monitoreo	
2018/10/09 09:22:56	2018/10/09 12:02:19	10.10.10.10	49722	9.9.9.9 FR	443	6	1,141 1,668	monitoreo	
2018/10/09 09:22:56	2018/10/09 11:54:58	10.10.10.10	49722	9.9.9.9 FR	443	4	0 264	monitoreo	
2018/10/09 09:22:56	2018/10/09 09:59:31	10.10.10.10	49722	9.9.9.9 FR	443	856	155,102 212,598	monitoreo	
2018/10/09 09:22:56	2018/10/09 10:19:38	10.10.10.10	49722	9.9.9.9 FR	443	4	0 264	monitoreo	
2018/10/09 09:22:56	2018/10/09 10:44:40	10.10.10.10	49722	9.9.9.9 FR	443	4	0 264	monitoreo	
2018/10/09 09:22:56	2018/10/09 11:09:46	10.10.10.10	49722	9.9.9.9 FR	443	6	0 396	monitoreo	
2018/10/09 09:22:56	2018/10/09 11:19:47	10.10.10.10	49722	9.9.9.9 FR	443	4	0 264	monitoreo	

Fuente: La investigación
Elaborado por: Autor

Ilustración 71: Muestra de contenido de paquete obtenido durante ejecución de "softwareCorporativo.py"

Fuente: La investigación
Elaborado por: Autor

4.5. Discusión de resultados.

4.5.1. Discusión de ETAPA UNO: Identificación de Topología Corporativa.

Al definir las cualidades necesarias y suficientes para el levantamiento de un laboratorio de análisis de malware, debe de considerar las características pertinentes de la red empresarial u organizacional de estudio y definir sus componentes críticos. Una topología de red empresarial «nivel mili» expuesta por Sridhar Iyer [34], posee propiedades aplicables a empresas medianas, pequeñas (PYMES) o sucursales de grandes corporaciones, cuales por lo general carecen de personal especializado en seguridad de información o responsables de la integridad del sistema, siendo propensos a vulnerabilidades de día cero, ataques masivos, ingeniería social, etc.

Los recursos necesarios (hardware) para virtualizar una topología de red completa, dependen directamente de la cantidad y capacidad de componentes conformantes del sistema. Por ello, es crucial la división de red en diferentes componentes con posibilidades de abstracción a un elemento mínimo sin afectaciones operativas, resaltando el rol importante de los componentes Intranet, DMZ, Firewall-router e Internet, pertenecientes a topología empresarial de amplia utilización y la agregación del componente Monitoreo con papel primordial en realización de análisis dinámico y el estudio tanto de la red en conjunto como por elementos independientes.

4.5.2. Discusión de ETAPA DOS: Virtualización de topología.

La importancia en elección de plataforma y técnica de virtualización radica en las posibilidades, distribución de recursos, seguridad, confiabilidad y soporte necesario para levantamiento de laboratorio aislado de análisis de malware. Para aprovechar la mayoría de recursos físicos disponibles en un equipo de virtualización dedicado es necesario la implementación de plataforma con arquitectura hipervisora como Proxmox, cual comparte correctamente el cien por ciento de los recursos y permite aplicación de tecnologías de virtualización con distintas posibilidades.

La técnica LXC, comparte el núcleo del sistema hipervisor (Linux) requiriendo menores recursos designados al momento de ejecución, ampliando el número de máquinas virtuales. Esta tecnología carece de aislación completa y trabaja directamente con el sistema operativo, involucrando cierto riesgo, también cuenta con limitaciones de aplicaciones

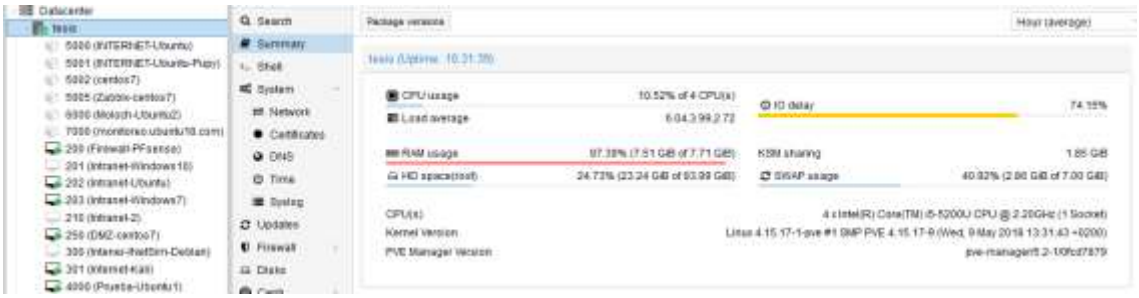
(compartir el mismo núcleo del hipervisor) y posibilidades reducidas. Las propiedades de ahorro de recursos y sus limitaciones de potencia y seguridad, hace factible la implementación de componentes no destinados a ejecución de malware pero necesarios para el funcionamiento de la red y monitoreo de sistemas.

La tecnología KVM, divide los recursos y aísla las máquinas virtualizadas, posibilitando implementar gran cantidad de sistemas operativos haciendo uso entero de recursos establecidos en configuración, permite una mayor seguridad, aislamiento y realismo, características requeridas para instauración de componentes con ejecución de malware (componente Intranet y DMZ). ***Ilustración 72*** muestra ejecución de topología usando tecnología LXC y KVM, mientras, ***Ilustración 73*** expresa el empleo de igual número de máquinas virtuales únicamente con KVM.

Ilustración 72: Ejecución de topología con técnicas LXC-KVM

Fuente: La Investigación
Elaborado por: Autor

Ilustración 73: Ejecución de topología únicamente con tecnología KVM



Fuente: La Investigación
Elaborado por: Autor

4.5.3. Discusión de ETAPA TRES: Identificación de muestras.

Las organizaciones son acechadas constantemente por distinto tipos de amenazas cibernéticas, los malware son el medio de ataque más común y potencialmente peligrosos para cualquier sistema. Según el propósito y alcance esperado, el software malicioso puede

clasificarse en malware masivo y malware dirigido; el primero es común en sistemas de gran difusión, como sistemas operativos de computadoras de escritorios o estaciones de trabajos en redes internas empresariales, debido a la extensa implementación del sistema operativo Windows 7, es uno de los sistemas con mayor existencia de malware a nivel mundial. Muestras de código malicioso (como "wayne.exe") pueden ser obtenidas de grandes base de datos mundiales destinadas a investigación, como «Hybrid-Analysis» o «VirusTotal».

Los códigos malignos dirigidos, están creados por profesionales pocos éticos de los sistemas objetivos, expresamente diseñados para explotar características propias de las redes víctimas, volviéndose gran preocupación para ingenieros de networking y responsables de seguridad informáticas. Existen generadores de software como Pupy (herramienta de acceso remoto), brindada al público con fines éticos (investigación y educación) pero con gran potencial para la creación y control de malware dirigido.

4.5.4. Discusión de ETAPA CUATRO: Análisis dinámico de malware.

Los registros obtenidos por software de monitoreo y de captura de paquetes empleados tanto en análisis de red completa como en sus componentes individuales, sirven de indicadores para inferir o afirmar comportamiento de malware. Los protocolos de Internet emulados por INetSim, son útiles en análisis inicial de archivos sospechosos, pudiendo indicar peticiones anómalas y guardando registros de los mismos. No obstante, cuando el malware requiere información específica para su correcta ejecución, es necesario la salida a Internet real, tomando las debidas precauciones.

El sistema de monitoreo y gráficas de rendimiento interno del sistema operativo «zabbix» indica variaciones menores respecto al malware "wayne.exe" ejecutado en componente Intranet, información no sustancial para deducir su comportamiento y afectación al sistema. Sin embargo, es usual encontrar código malicioso con poca afectación a los recursos locales, por motivos de ocultamiento, usual en malware tipo spyware. El rendimiento del componente DMZ durante análisis dinámico de "softwareCorporativo.py", ocurre en momentos puntuales durante ejecución de comandos de explotación desde el servidor RAT remoto, sobresaliente de un sistema con rendimiento constante y carga inusual de cpu, ram y tráfico elevado de red.

Las herramientas usadas para capturar paquetes «Moloch» y «daemonlogger», permite realizar sniffing en redes virtuales, obteniendo los paquetes cursados por distintas redes, al conocer las conexiones usuales, puede tomarse como punto de partida en caso de anomalías

de intentos de conexión remota. La muestra “wayne.exe” posee peticiones remotas a servidores externos y consultas a «checkip.dyndns.org» realizadas al momento de ejecución del espécimen, en tiempo posterior, posee transferencia inusuales a «smtp.zoho.com» con carga vacía, no obstante puede servir de aviso o reporte a servidores remotos de control, advirtiendo del contagio y disponibilidad de realizar post-explotación. El espécimen “softwareCorporativo.py” posee conexiones esperadas según la creación expresa del RAT (9.9.9.9) no obstante, sus paquetes cuentan con cifrado SSL, imposibilitando de forma externa, obtener la información contenida.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones.

- Los componentes de una topología de seguridad perimetral empleando una zona desmilitarizada, red interna, firewall-router e internet pueden ser abstraídos en elementos básicos, conservando la funcionalidad y operatividad de una red completa, posibilitando su estudio. La componente Intranet con un sistema operativo de amplio uso, corre el riesgo de infección por malware masivo, no obstante, los sistemas pertenecientes al componente DMZ, suelen ser objetivos de malware dirigido específicamente diseñado para transgredir particularidades.
- La aplicación de tecnología de virtualización «LXC» y «KVM» según la finalidad e importancia de aislamiento en componentes, permite virtualizar redes con mayor cantidad de elementos salvaguardando los recursos físicos del servidor de virtualización. Para crear diferentes redes separadas e interconexión de máquinas virtuales, es suficiente con la utilización de switch virtuales y la correcta configuración de tarjetas de red.
- El hipervisor «Proxmox», facilita la interconexión de los componentes, permitiendo la configuración eficiente de la topología establecida. El empleo de una red de aislamiento completo con el uso de «INetSim» como servicio de emulación de protocolos comunes de Internet, permite un primer acercamiento sobre las funcionalidades de las muestras, no obstante, es necesaria la salida real a internet para mejorar resultados. Existe limitaciones en evaluación de elementos virtuales con herramientas externas; el software de monitoreo «Zabbix», permite obtener gráficas de rendimiento, sin embargo, el cambio en la utilización de recursos debe de ser en extremo abrupto, para notar diferencias. «Moloch» permite la captura de paquetes de varias redes simultáneas, imposibilitado de comprender la carga útil de conexiones cifradas.

5.2. Recomendaciones.

- Categorizar, dividir y abstraer en unidades elementales, distintos tipos y complejidades de topologías corporativas, constando con el tamaño de la organización y los servicios soportados por su red, sin afectar la operatividad de la misma, con el fin de salvaguardar los recursos de virtualización, tomando a consideración el funcionamiento de la red en general. Es posible la emulación completa de una red corporativa real, contando con la información necesaria, y efectuar análisis de vulnerabilidades o planear respuestas ante infiltraciones de malware en sistemas sensibles.
- Realizar categorización de elementos abstraídos de acuerdo a la importancia de aislamiento o potencia de recursos necesarios, con el fin de elección sobre tecnología de virtualización a aplicar (KVM o LXC). La simplificación de topologías de red para su virtualización, permite el análisis del sistema según diversos objetivos: búsqueda de vulnerabilidades, prueba preliminar de nuevas configuraciones, estudio de puntos críticos, delimitación de dominio de fallos, etc.
- Verificar el correcto hermetismo de topología virtual previo a ejecución de muestras, para impedir una fácil propagación a otros sistemas en caso de poseer comportamiento de gusanos. El estudio con salida real a Internet debe de realizarse con las debidas precauciones para mantener el anonimato de origen, no levantar sospecha de atacantes externos y minimizar riesgo para la infraestructura real en donde se desarrolle la investigación.

CAPÍTULO VI

BIBLIOGRAFÍA

Bibliografía

[1] Eset latinoaméria , «eset security report latinoamerica 2017,» 2017.

[2] Arielmcorg, «infosertec.com.ar,» 5 4 2018. [en línea]. Available: https://infosertec.com.ar/2018/04/05/informe-el-70-de-los-usuarios-cree-que-los-dispositivos-iot-no-son-seguros/. [último acceso: 24 5 2018].

[3] Latam.kaspersky.com, «latam.kaspersky.com,» 2018. [en línea]. Available: https://latam.kaspersky.com/resource-center/definitions/metamorphic-virus. [último acceso: 24 5 2018].

[4] Eset, «empresas.eset-la.com,» 2018. [en línea]. Available: https://empresas.eset-la.com/archivos/novedades/69/eset_security_report_latam2018-final.pdf. [último acceso: 2018].

[5] L. Zeltser, «digital-forensics.sans.org,» 29 7 2014. [en línea]. Available: https://digital-forensics.sans.org/blog/2014/07/29/etapas-del-analisis-de-malware. [último acceso: 24 5 2018].

[6] Cisco networking academy, network basics companion guide, indianapolis: ciscon press, 2014.

[7] Cisco systems, ccna: intoducción a las redes v.6.0, indianapolis: cisco press, 2017.

[8] Univsersidad de valencia , sistema industriales distribuidos, valencia - españa: universidad de valencia.

[9] A. S. Iyer, «introduction to enterprise networks:,» de *iit bombay - convergencia* , bombay, 2005.

[10] Wikipedia.org, «wikipedia,» [en línea]. Available: https://es.wikipedia.org/wiki/virtualizaci%c3%b3n. [último acceso: 12 6 2018].

[11] F. R. S. V. Jorge xavier andrade sarmiento, estudio e implementación de una solución de virtualización para la universidad politécnica salesiana, guayaquil - ecuador: universidad politécnica salesiana, 2012.

[12] Ivan ramirez, «xataca.com,» 4 8 2016. [en línea]. Available: https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas. [último acceso: 5 6 2018].

[13] C. Z. S., «la virtualización, tipos de virtualizaciones,» universidad ecotec, 2012.

[14] R. Velazco, «softone.es,» 14 3 2017. [en línea]. Available: https://www.softzone.es/2017/03/14/comparativa-vmware-virtualbox/. [último acceso: 5 6 2018].

[15] Proxmox server solutions gmbh, «proxmox.com,» 2018. [en línea]. Available: https://www.proxmox.com/en/proxmox-ve. [último acceso: 2018].

[16] Wikipedia, «wikipedi,» [en línea]. Available: https://es.wikipedia.org/wiki/windows_virtual_pc. [último acceso: 5 6 2018].

[17] H. R. P. Valdivieso, implementación de un sistema de gestión central y unificada sobre seguridad en ambientes microsoft en el laboratorio de tecnologías de información y comunicación (ltic) de la facultad de ingeniería., guayaquil - ecuador: pontificia universidad católica del ecuador, 2010.

[18] G. J. L. Cheng, análisis estático y dinámico de una muestra de malware en sisteas microsoft windows xp para determinar que efectos produce sobre un sistema infectado, quit: escuela politécnica nacional, 2014.

[19] C. A. Aramburu, metodología de análisis de malware al caso de estudio de la amenaza avanzada persistente (apt) "octubre rojo", 2015.

[20] J. Bermejo, desarrollo de un sistema de análisis e ingeniería inversa de código malicioso, 2015.

[21] P. A. Gaviria, aplicación de metodología de malware para el análisis de la amenaza avanzada persistente (apt) "poison ivy", bogotá: universidad internacional de la rioja, 2016.

[22] I. L. R. C. Henry cristhian mancheno torres, vulnerabilidades y seguridad en redes tcp/ip, guayaquil-ecuador: universidad católica de santiago de guayaquil, 2013.

[23] A. H. Michael sikorski, «practical malware analysis. The hans-on guide to dissectin malicious software,» no starch press, san francisco, 2012.

[24] D. F. A. Villaruel, análisis digital de una infección de malware en sistemas windows, quito: escuela politécnica nacional, 2016.

[25] S. O. Fernández, análisis dinámico de malware ne entornos controlados, madrid: universidad carlos iii de madrid, 2013.

[26] T. M. J. Tene, metodología para el análisis de malware en un ambiente controlado, cuenca: universidad politécnica salesiana sede cuenca , 2017.

[27] Kaspersky, «support.kaspersky.com,» 2018. [en línea]. Available: https://support.kaspersky.com/mx/789#block2. [último acceso: 5 23 2018].

[28] Cisco, «introducción a la ciberseguridad,» cisco, 2018.

[29] Y. P. I. R. Syarif yusirwan s, «implementation of malware analysis using static and dynamic analysis method,» *international journal of computer applications (0975 – 8887)*, vol. 117, nº 6, 2015.

[30] A. Sanabria, «malware analysis: environment design and artitecture,» sans institute, 2007.

[31] Vmware.com, «esxi and vcenter server 5.1 documentation,» [en línea]. Available: https://pubs.vmware.com/vsphere-51/index.jsp?Topic=%2fcom.vmware.vsphere.vm_admin.doc%2fguid-ceff6d89-8c19-4143-8c26-4b6d6734d2cb.html. [último acceso: 24 5 2018].

[32] Dicionario de la real academia española, «http://dle.rae.es,» 2018. [en línea]. Available: http://dle.rae.es/srv/fetch?Id=esut8fg. [último acceso: 07 27 2018].

[33] L. Vargas, «importancia de las empresas en la economía,» 3 3 2015. [en línea]. Available: https://www.larepublica.net/noticia/importancia_de_las_empresas_en_la_economia. [último acceso: 27 7 2018].

[34] I. Sridhar, «introduction to enterprise networks:,» de *iit bombay - convergencia*, bombay, 2005.

[35] T. Cross, «stealthwatch & point-of-sale (pos) malware,» de *lancope*, 2018.

[36] Tp-link, «www.tp-link.com,» 29 11 2011. [en línea]. Available: https://www.tp-link.com/es/faq-28.html. [último acceso: 28 7 2018].

[37] M. Porolli, «welivesecurity,» copyright © eset, 10 7 2013. [en línea]. Available: https://www.welivesecurity.com/la-es/2013/07/10/utilizando-inetsim-analisis-dinamico-malware/.

[38] V. Mohan, a guide to enterprise network monitoring, solarwinds worldwide, llc., 2015.

[39] A. Cecil, «a summary of network traffic monitoring and analysis,» cse.wustl.edu, 2006.

[40] I.t.now, «itnow.net,» i.t.now, 8 10 2015. [en línea]. Available: https://itnow.net/the-importance-of-network-monitoring/. [último acceso: 3 10 2018].

[41] S. C. Rakesh kumar, «an importance of using virtualization technology in cloud computing,» de *global journal of computers & technology* , jaipur - india, 2015.

[42] Pve.proxmox.com, «pve.proxmox.com,» 17 07 2017. [en línea]. Available: https://pve.proxmox.com/wiki/system_requirements. [último acceso: 30 07 2018].

[43] Universidad de indiana, «kb.iu.edu,» universidad de indiana, 18 01 2018. [en línea]. Available: https://kb.iu.edu/d/amxs. [último acceso: 31 07 2018].

[44] J. P. Andrés, «debianitas.net,» 20 10 2014. [en línea]. Available: http://www.debianitas.net/libros/proxmox/proxmox-requisitos. [último acceso: 31 07 2018].

[45] Pve.proxmox.com, «pve.proxmox.com,» 16 05 2018. [en línea]. Available: https://pve.proxmox.com/wiki/install_from_usb_stick. [último acceso: 30 07 2018].

[46] Proxmoxve, «pve.proxmox.com,» 16 05 2018. [en línea]. Available: https://pve.proxmox.com/wiki/network_configuration. [último acceso: 31 7 2018].

[47] Qre0ct, «security.stackexchange.com,» 17 08 2016. [en línea]. Available: https://security.stackexchange.com/questions/134111/inetsim-installation-perlipq-libipq-error. [último acceso: 1 08 2018].

[48] Rubicon communications llc, «netgate.com,» [en línea]. Available: https://www.netgate.com/docs/pfsense/config/example-basic-configuration.html. [último acceso: 1 08 2018].

[49] Hybrid-analysis.com, «hybrid-analysis.com,» 2018. [en línea]. Available: https://www.hybrid-analysis.com/. [último acceso: 2018].

[50] C. Cimpanu, «bleepingcomputer.com,» 18 06 2018. [en línea]. Available: https://www.bleepingcomputer.com/news/security/75-percent-of-malware-uploaded-on-no-distribute-scanners-is-unknown-to-researchers/. [último acceso: 2018].

[51] Windowsreinstall.com, «windowsreinstall.com,» [en línea]. Available: http://windows7.windowsreinstall.com/systemrequirements.htm. [último acceso: 30 07 2018].

[52] Help.ubuntu.com, «ubuntu.com,» 13 10 2017. [en línea]. Available: https://help.ubuntu.com/community/installation/systemrequirements. [último acceso: 30 07 2018].

[53] Redhat.com, «access.redhat.com,» [en línea]. Available: https://access.redhat.com/documentation/en-us/red_hat_directory_server/9.0/html/installation_guide/platform_support. [último acceso: 30 07 2018].

[54] Pfsense, «pfsense.org,» [en línea]. Available: https://www.pfsense.org/products/. [último acceso: 30 07 2018].

[55] C. E. M. Álvarez, metodología: diseño y desarrollo del proceso de investigación con énfasis en ciencias empresariales, méxico d.f: limusa, 2011.

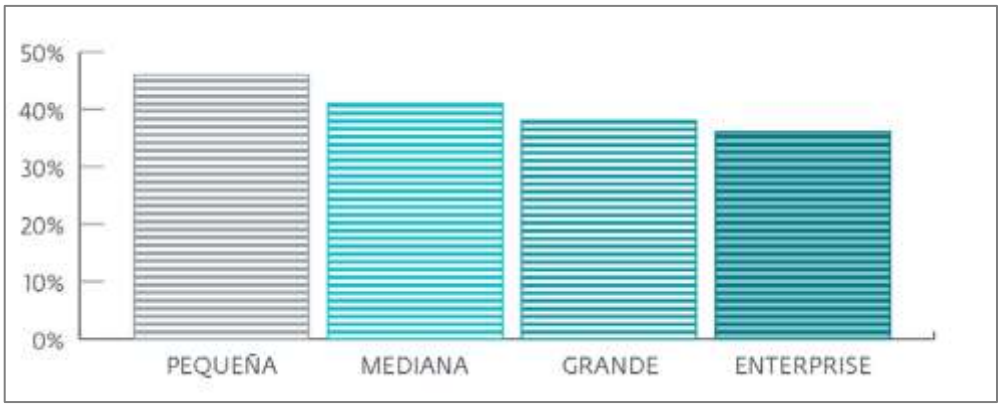
CAPÍTULO VII

ANEXOS

Anexo 1: Infecciones de malware por país

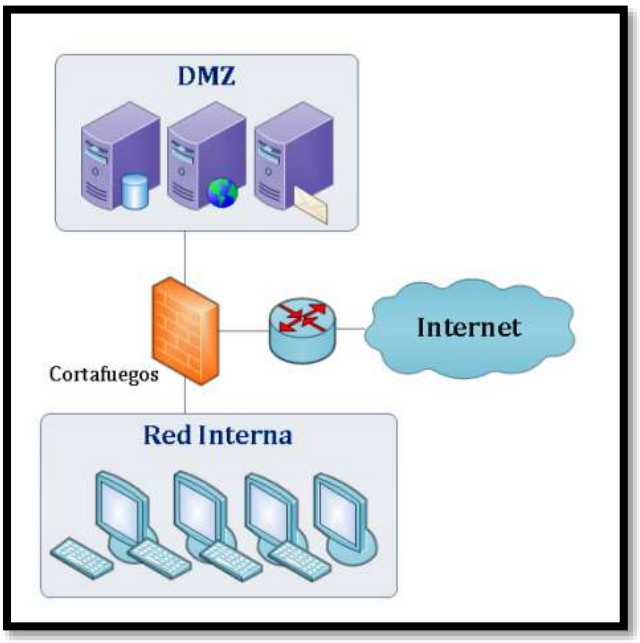
Fuente: ESET-LATAM
Elaborado por: ESET-LATAM

Anexo 2: Porcentaje de empresas que dijeron no tener incidentes de seguridad durante los últimos 12 meses por tamaño de empresa.



Fuente: ESET-LATAM
Elaborado por: ESET-LATAM

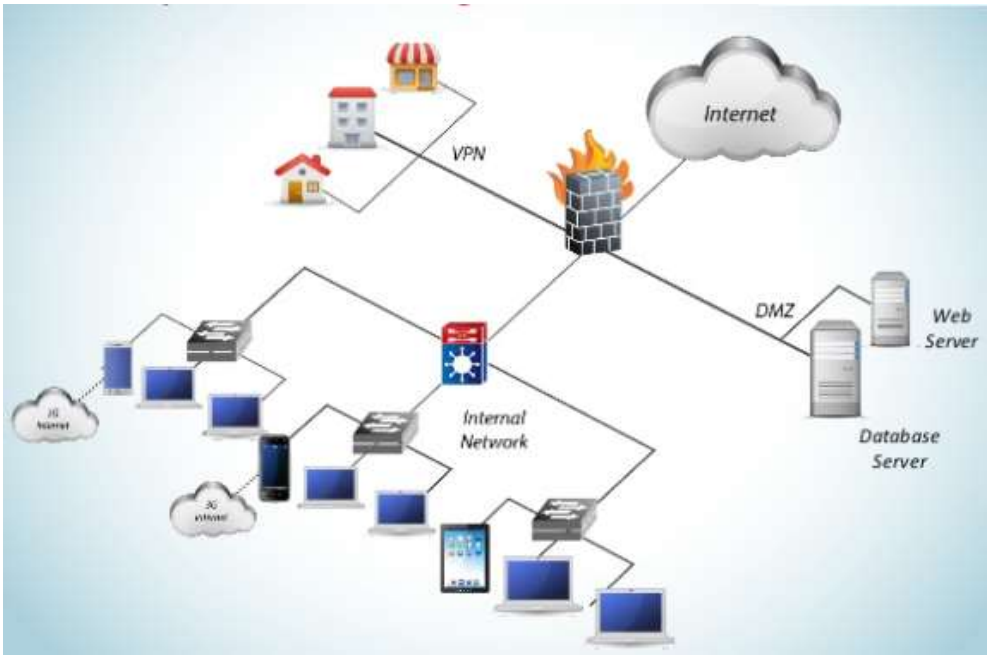
Anexo 3: Topología de seguridad perimetral de amplio uso empleando una DMZ con un cortafuego en trípode.



Fuente: criptored.upm.es[61]
Elaborado por: Autor

/

Anexo 4: Diagrama de red corporativa básica.



Fuente: Lancoupe[62]
Elaborado por: Tom Cross

[61] http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf
[62] https://www.slideshare.net/Lancope/retailwebinar

Anexo 5: Encuesta realizada por la «StatCounter Global Stats reports»

Fuente: gs.statcounter.com[63]
Elaborado por: Autor

Anexo 6: Estadísticas reflejadas en «netmarketshare.com»

Fuente: bleepingcomputer.com[64]
Elaborado por: Autor

[63] http://gs.statcounter.com/os-market-share#monthly-201708-201709-bar

[64] https://www.bleepingcomputer.com/news/microsoft/windows-10-overtakes-windows-7-to-become-most-popular-windows-version/

Anexo 7: Estadísticas de w3techs.com sobre liderazgo de Linux

Fuente: w3techs.com[65]
Elaborado por: Autor

Anexo 8: Importancia del mercado del servidor web Apache por news.netcraft.com

Developer	August 2017	Percent	September 2017	Percent	Change
Apache	77,916,218	44.99%	77,487,531	44.89%	-0.10
nginx	35,566,579	20.54%	35,640,320	20.65%	0.11
Google	13,379,490	7.72%	13,561,655	7.86%	0.13
Microsoft	13,136,286	7.58%	12,629,582	7.32%	-0.27

Fuente: news.netcraft.com[66]
Elaborado por: Autor

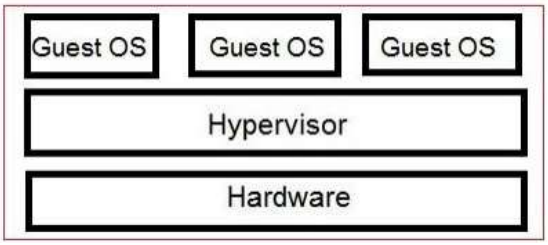
[65] https://w3techs.com/technologies/comparison/os-linux,os-windows

[66] https://news.netcraft.com/archives/2017/09/11/september-2017-web-server-survey.html

Anexo 9: Ranking expuesto hasta junio de 2018 por «itcentralstation.com» sobre firewalls más usados

Fuente: itcentralstation.com[67]
Elaborado por: Autor

Anexo 10: Arquitectura de virtualización con Hipervisor.



Fuente: ResearchGate[68]
Elaborado por: Rakesh Kumar y Shilpi Charu

[67] https://www.itcentralstation.com/categories/firewalls
[68] https://www.researchgate.net/publication/273723426

Anexo 11: Estadísticas de frecuencia de investigación para softwares de virtualización de servidores

Fuente: trustradius.com[69]
Elaborado por: Autor

Anexo 12: Especificación de versión, medio de instalación y arquitectura de CPU para instalación de pfsense

Fuente: pfsense.org[70]
Elaborado por: Autor

[69] https://www.trustradius.com/server-virtualization

[70] https://www.pfsense.org/download/

Anexo 13: Servicios brindados por InetSim

Fuente: inetsim.org[71]
Elaborado por: Autor

Anexo 14: Requerimientos de Pupy

```
root@INTERNET-Ubuntu-Pupy:~/pupy/pupy# cat requirements.txt
tinyec
psutil
netifaces
pylzma
mss==2.0.22
colorama
pyOpenSSL
scapy
impacket
pyuv
dnslib
http-parser
cerberus
logutils
secretstorage
pygments
requests
keyboard
```

Fuente: La Investigación
Elaborado por: Autor

[71] https://www.inetsim.org/requirements.html

Anexo 15: Manual de levantamiento de servidor Apache en Componente DMZ

1) Instalar servidor httpd y realizar levantación de servicio

```
[root@localhost ~]# yum install httpd -y
[root@localhost ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@localhost ~]#
```

2) Crear los archivos respectivos y página html a mostrar

```
[root@localhost ~]# mkdir -p /var/www/analisisdemalware.com/public_html
[root@localhost ~]# chmod -R 755 /var/www
```

```
  GNU nano 2.3.1                Fichero: /var/www/analisisdemalware.com/public                Modificado

<html>
        <head>
                <title> SERVIDOR DMZ </tittle>
        </head>
        <body>
           <h1> ESTA DENTRO DE LA WEB DEL SERVIDOR DMZ, FELICIDADES </h1>
        </body>
</html>_
```

3) Crear archivos para aplicación de virtual hostst y configurar httpd.conf según lo mostrado en la ilustración.

```
[root@localhost ~]# mkdir /etc/httpd/sites-available
[root@localhost ~]# mkdir /etc/httpd/sites-enabled
  GNU nano 2.3.1                Fichero: /etc/httpd/conf/httpd.conf                Mod

# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#

#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files.  This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
IncludeOptional sites-enabled/*.conf
```

4) Por cuestiones de análisis de malware, se recomienda desactivar «selinux» y firewall de Linux. Al finalizar es necesario reiniciar el servicio 'apachectl restart'

```
  GNU nano 2.3.1                Fichero: /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

```
[root@localhost www]# setenforce 0_
```

```
[root@localhost network-scripts]# service firewalld stop
Redirecting to /bin/systemctl stop firewalld.service
[root@localhost network-scripts]# systemctl disable firewalld_
```

Anexo 16: Manual de Instalación de Moloch

1) Añadir los repositorios necesarios, instalar dependencias incluida java 8, y desactivar el empleo del swap

```
root@monitoreo:~# add-apt-repository ppa:webupd8team/java
root@monitoreo:~# apt-get update
root@monitoreo:~# apt-get install zip && apt-get install npm
root@monitoreo:~# apt-get install oracle-java8-installer
root@monitoreo:~# apt-get install oracle-java8-installer
```

2) Verificar la configuración de red, en donde eth2 servirá para sniffear redes

```
  GNU nano 2.9.3                  /etc/network/interfaces                  Modified

# ifupdown has been replaced by netplan(5) on this system.  See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
#    sudo apt install ifupdown
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.1.39
        netmask 255.255.255.0
        gateway 192.168.1.1
auto eth1
iface eth1 inet static
        address 172.16.0.1
        netmask 255.255.255.0
up route add -net 192.168.100.0 netmask 255.255.255.0 gw 172.16.0.2
up route add -net 10.10.10.10 netmask 255.255.255.255 gw 172.16.0.2

auto eth2
iface eth2 inet manual
ethool -G eth1 rx 4096 tx 4096
ethool -K eth1 rx off tx off gs off tso off gso off
```

3) Descargar «Moloch» y «ElasticSearch»

```
root@monitoreo:~# wget https://files.molo.ch/builds/ubuntu-18.04/moloch-nightly_amd64.deb
--2018-08-25 22:23:13--  https://files.molo.ch/builds/ubuntu-18.04/moloch-nightly_amd64.deb
Resolving files.molo.ch (files.molo.ch)... 54.192.81.249, 54.192.81.77, 54.192.81.57, ...
Connecting to files.molo.ch (files.molo.ch)|54.192.81.249|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 83539456 (80M) [binary/octet-stream]
Saving to: 'moloch-nightly_amd64.deb'

moloch-nightly_amd64.de 100%[=============================>]  79.67M   738KB/s    in 1m 40s

2018-08-25 22:24:54 (816 KB/s) - 'moloch-nightly_amd64.deb' saved [83539456/83539456]

root@monitoreo:~# ls
moloch-nightly_amd64.deb
root@monitoreo:~# wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.6.
11.deb
```

4) Instalar Moloch-nightly y sus dependencias

```
root@monitoreo:~# dpkg -i moloch-nightly_amd64.deb
Selecting previously unselected package moloch-nightly.
(Reading database ... 36685 files and directories currently installed.)
Preparing to unpack moloch-nightly_amd64.deb ...
Unpacking moloch-nightly (1.5.3-GIT-755) ...
dpkg: dependency problems prevent configuration of moloch-nightly:
 moloch-nightly depends on libwww-perl; however:
  Package libwww-perl is not installed.
 moloch-nightly depends on libjson-perl; however:
  Package libjson-perl is not installed.
 moloch-nightly depends on ethtool; however:
  Package ethtool is not installed.
 moloch-nightly depends on libyaml-dev; however:
  Package libyaml-dev is not installed.
root@monitoreo:~# apt-get -f install
```

5) Instalar «ElasticSearch» y mover archivo .yml y reiniciar servicio

```
root@monitoreo:~# systemctl start elasticsearch.service
root@monitoreo:~# systemctl status elasticsearch.service
* elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; vendor preset: ena
   Active: active (running) since Sat 2018-08-25 22:39:57 UTC; 36s ago
     Docs: http://www.elastic.co
  Process: 12145 ExecStartPre=/usr/share/elasticsearch/bin/elasticsearch-systemd-pre-exec (cod
 Main PID: 12146 (java)
    Tasks: 17 (limit: 4915)
   CGroup: /system.slice/elasticsearch.service
           `-12146 /usr/bin/java -Xms2g -Xmx2g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupa

root@monitoreo:~# cd /etc/elasticsearch
root@monitoreo:/etc/elasticsearch# ls
elasticsearch.yml  jvm.options  log4j2.properties  scripts
root@monitoreo:/etc/elasticsearch# mv elasticsearch.yml elasticsearch.yml.bkg

root@monitoreo:/etc/elasticsearch# systemctl restart elasticsearch.service
```

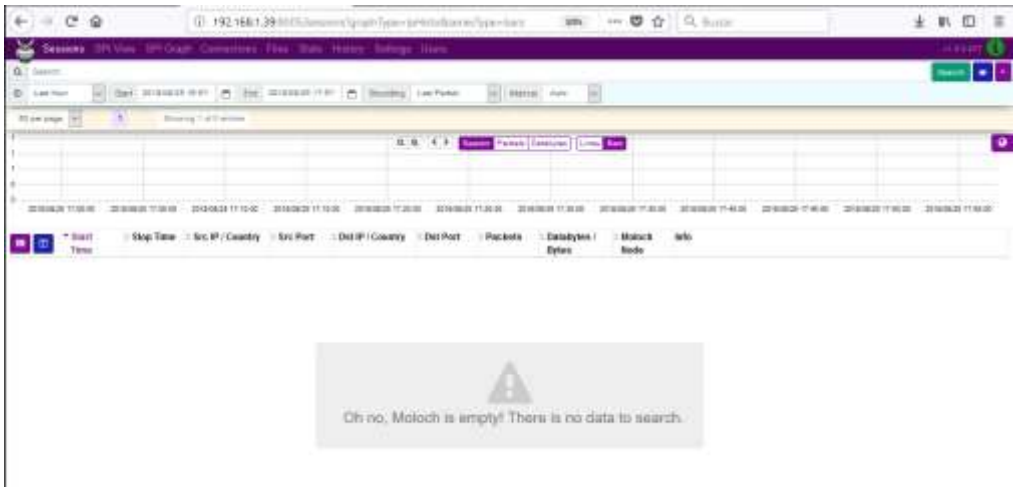
6) Inicializar base de datos y agregar usuario.

```
root@monitoreo:/etc/elasticsearch# /data/moloch-nightly/db/db.pl http://localhost:9200 init
It is STRONGLY recommended that you stop ALL moloch captures and viewers before proceeding.

There is 1 elastic search data node, if you expect more please fix first before proceeding.

This is a fresh Moloch install
Erasing
Creating


Finished
root@monitoreo:~# /data/moloch-nightly/bin/moloch_add_user.sh moloch moloch tesis --admin
Added
```

7) Encender servicios «molochviewer» para acceder al web-client de Moloch, y «molochcapture» para iniciar escucha de paquetes

```
root@monitoreo:~# systemctl start molochcapture
root@monitoreo:~# systemctl start molochviewer
root@monitoreo:~# ufw allow 8005/tcp
Rule added
Rule added (v6)
```

8) Ya es posible acceder al web-cliente con el usuario creado con anterioridad.



Anexo 17: Manual de instalación de servidor Zabbix

1) Instalar Y configurar servidor web apache.

```
root@monitoreo:~# apt-get install apache2
```

```
  GNU nano 2.9.3                /etc/apache2/conf-enabled/security.conf

# Changing the following options will not really affect the security of the
# server, but might make attacks slightly more difficult in some cases.

#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full
root@monitoreo:~# systemctl restart apache2
```

2) Instalar y configurar php

```
root@monitoreo:~# apt-get -y install php php-pear php-cgi php-common libapache2-mod-php \
hp-gd > php-mbstring php-net-socket php-gd php-xml-util php-mysql php-gettext php-bcmath

root@monitoreo:~# php -v
PHP 7.2.7-0ubuntu0.18.04.2 (cli) (built: Jul  4 2018 16:55:24) ( NTS )
Copyright (c) 1997-2018 The PHP Group
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
    with Zend OPcache v7.2.7-0ubuntu0.18.04.2, Copyright (c) 1999-2018, by Zend Technologies
root@monitoreo:~#
```

```
Enabling conf php7.2-cgi.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@monitoreo:~# systemctl reload apache2
root@monitoreo:~# a2enconf php7.2-cgi
Enabling conf php7.2-cgi.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@monitoreo:~# systemctl reload apache2
root@monitoreo:~# systemctl restart apache2
```

3) Instalar base de datos MariaDB

```
root@monitoreo:~# apt-get install software-properties-common
root@monitoreo:~# apt-key adv --recv-keys --keyserver hkp://keyserver.ubuntu.com:80 0xF1656F24
C74CD1D8
root@monitoreo:~# add-apt-repository 'deb [arch=amd64] http://mirror.zol.co.zw/mariadb/repo/10
.3/ubuntu bionic main'
root@monitoreo:~# apt-get update && apt-get -y install mariadb-server mariadb-client
```

4) Creamos base de datos “zabbix” con MariaDB

```
root@monitoreo:~#  mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 48
Server version: 10.3.9-MariaDB-1:10.3.9+maria~bionic-log mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> select version();
+-----------------------------------------+
| version()                               |
+-----------------------------------------+
| 10.3.9-MariaDB-1:10.3.9+maria~bionic-log |
+-----------------------------------------+
1 row in set (0.000 sec)

MariaDB [(none)]> create database zabbix;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@'localhost' identified by 'tesis'
;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> exit;
Bye
```

5) Instalamos repositorio para descarga de “zabbix” e instalamos los paquetes correspondientes

```
root@monitoreo:/media# wget http://repo.zabbix.com/zabbix/3.4/ubuntu/pool/main/z/zabbix-releas
e/zabbix-release_3.4-1+bionic_all.deb
--2018-08-24 21:46:30--  http://repo.zabbix.com/zabbix/3.4/ubuntu/pool/main/z/zabbix-release/z
abbix-release_3.4-1+bionic_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 162.243.159.138
Connecting to repo.zabbix.com (repo.zabbix.com)|162.243.159.138|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3952 (3.9K) [application/octet-stream]
Saving to: 'zabbix-release_3.4-1+bionic_all.deb'

zabbix-release_3.4-1+bi 100%[=============================>]   3.86K  --.-KB/s    in 0s

2018-08-24 21:46:30 (249 MB/s) - 'zabbix-release_3.4-1+bionic_all.deb' saved [3952/3952]

root@monitoreo:/media# ls
zabbix-release_3.4-1+bionic_all.deb
root@monitoreo:/media# dpkg -i zabbix-release_3.4-1+bionic_all.deb
root@monitoreo:/media# apt-get update && apt-get -y install zabbix-agent zabbix-server-mysql p
hp-mysql zabbix-frontend-php
```

6) Importamos base de datos y configuramos archivo “zabbix_server.conf”

```
  GNU nano 2.9.3                  /etc/zabbix/zabbix_server.conf

# DBUser=

DBUser=zabbix

### Option: DBPassword
#       Database password. Ignored for SQLite.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=tesis
```

```
root@monitoreo:~#  zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p z
abbix
Enter password:
root@monitoreo:~# systemctl restart zabbix-server.service
```

7) Modificamos archivo “CFrontendSetup.php” agregando $current = -1;

```
 GNU nano 2.9.3     /usr/share/zabbix/include/classes/setup/CFrontendSetup.php      Modified

        * Checks for PHP option always_populate_raw_post_data. As of PHP version 5.6.0 this$
        * In case this option is not set or is enabled, PHP will throw E_DEPRECATED error. $
        * ini php.ini and cannot be set at runtime.
        *
        * See: http://php.net/manual/en/ini.core.php#ini.always-populate-raw-post-data
        *
        * @return array
        */
       public function checkPhpAlwaysPopulateRawPostData() {
               $current = ini_get('always_populate_raw_post_data');
               $current = -1;
```

8) Modificamos configuración php con requerimientos de zabbix

```
 GNU nano 2.9.3                    /etc/php/7.2/apache2/php.ini                    Moc

; http://php.net/expose-php
expose_php = Off

;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;;

; Maximum execution time of each script, in seconds
; http://php.net/max-execution-time
; Note: This directive is hardcoded to 0 for the CLI SAPI
max_execution_time = 300
```

```
max_input_time = 300
post_max_size = 16M
```

9) Configuración de agente zabbix para equipo local

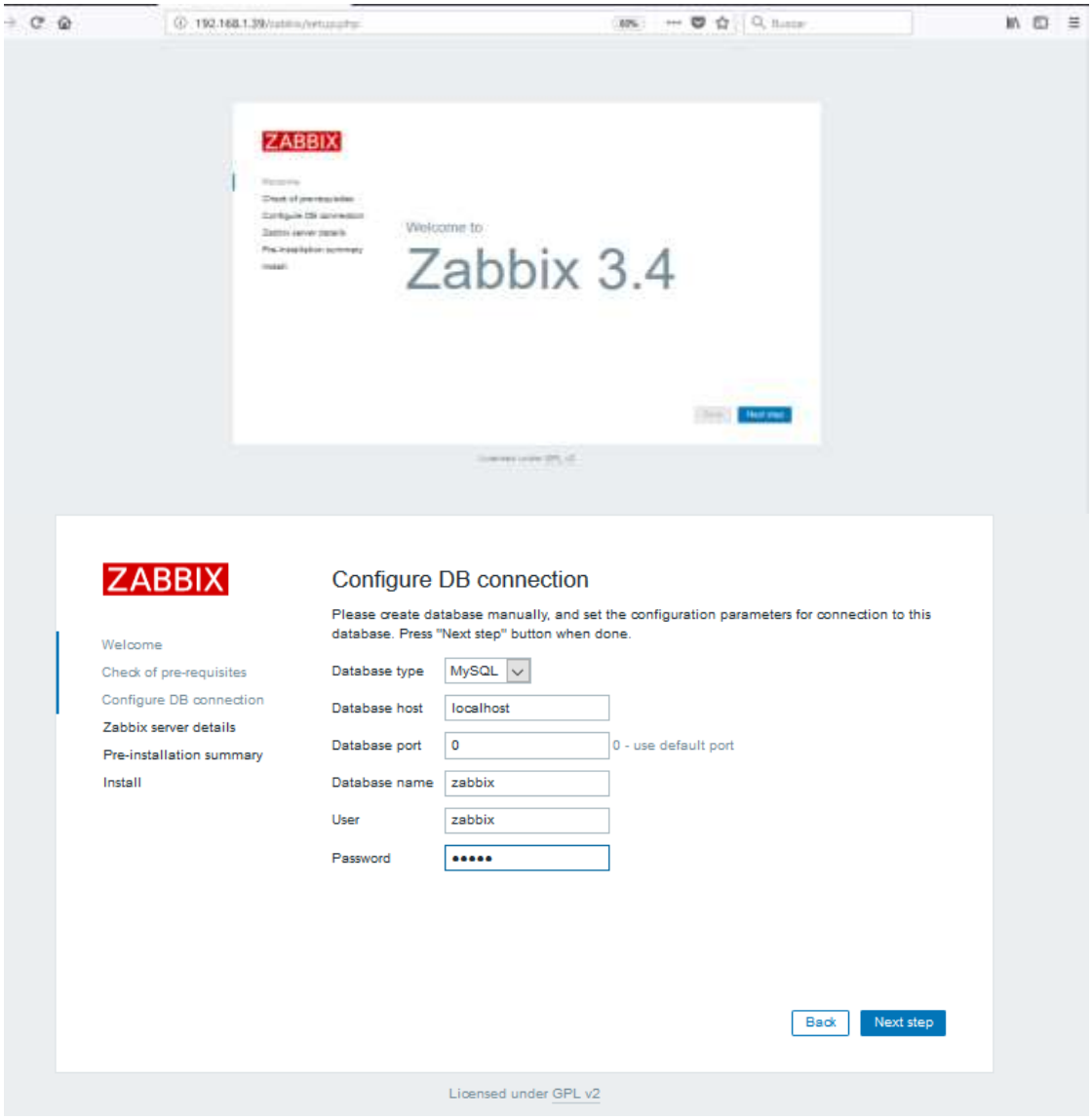
```
 GNU nano 2.9.3                  /etc/zabbix/zabbix_agentd.conf                  Modified

#       Unique, case sensitive hostname.
#       Required for active checks and must match hostname as configured on the server.
#       Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=

Hostname=monitoreo.ubuntu18.com
```

10) Agregamos las correspondientes reglas al firewall y reiniciamos servicios

```
root@monitoreo:~#  ufw enable
Firewall is active and enabled on system startup
root@monitoreo:~# ufw allow http
Rule added
Rule added (v6)
root@monitoreo:~# ufw allow https
Rule added
Rule added (v6)
root@monitoreo:~# ufw allow 10051/tcp
Rule added
Rule added (v6)
root@monitoreo:~# ufw allow  10050/tcp
Rule added
Rule added (v6)
```

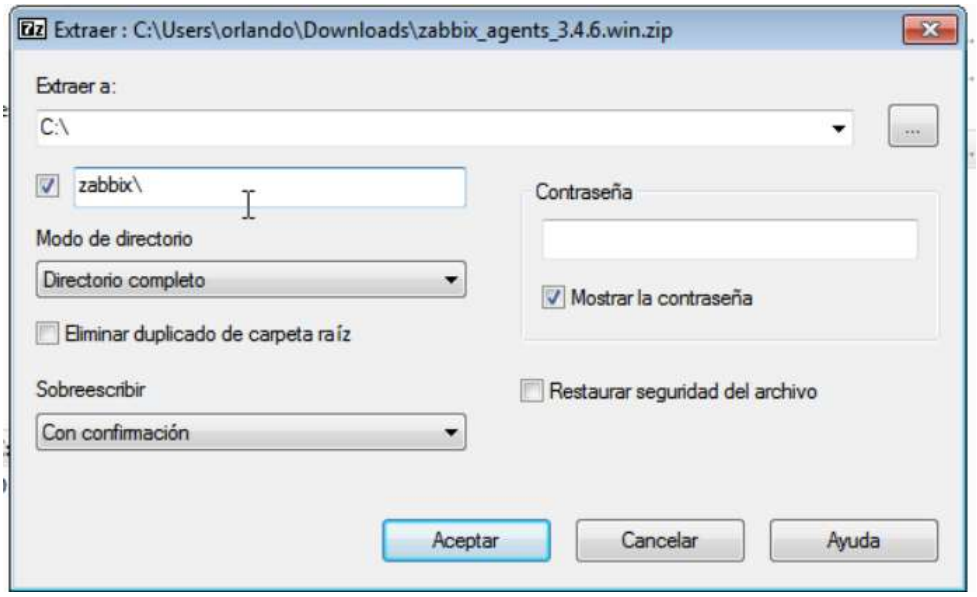
```
root@monitoreo:~# systemctl restart zabbix-server.service
root@monitoreo:~# systemctl restart zabbix-agent.service
root@monitoreo:~# systemctl enable zabbix-server.service
Synchronizing state of zabbix-server.service with SysV service script with /lib/systemd/system
d-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
root@monitoreo:~# systemctl enable zabbix-agent.service
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd
-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
root@monitoreo:~# systemctl restart apache2
```

9) El restante de la configuración se continúa mediante el web-client



Anexo 18: Manual de instalación de agente Zabbix en componente Intranet.

1) Descargar desde el sitio oficial: https://tecadmin.net/install-zabbix-agent-windows-system/
2) Extraemos en el disco C:



1) Copiar archivo “zabbix_agentd.win.conf” dentro de ruta “C://zabbix”

2) Modificar dicho archivo según especificaciones del servidor.

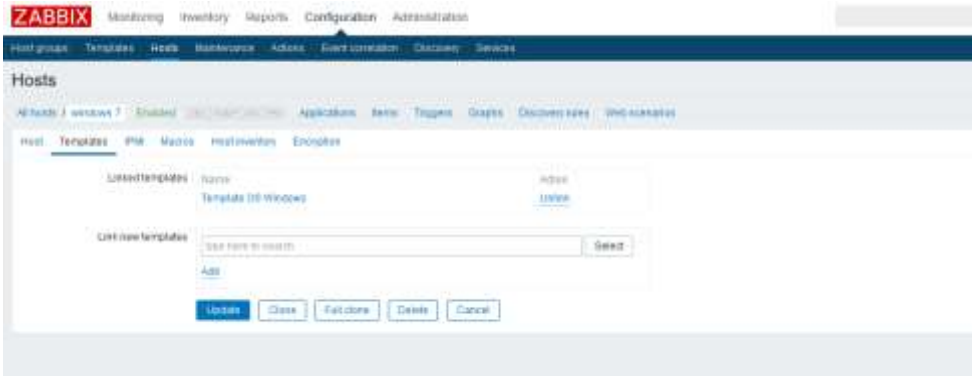
```
# Mandatory: no
# Default:
# Server=

Server=172.16.0.1

### Option: ListenPort
#    Agent will listen on this port for connections from the
server.
#
# Mandatory: no
# Range: 1024-32767
# Default:
# ListenPort=10050
```

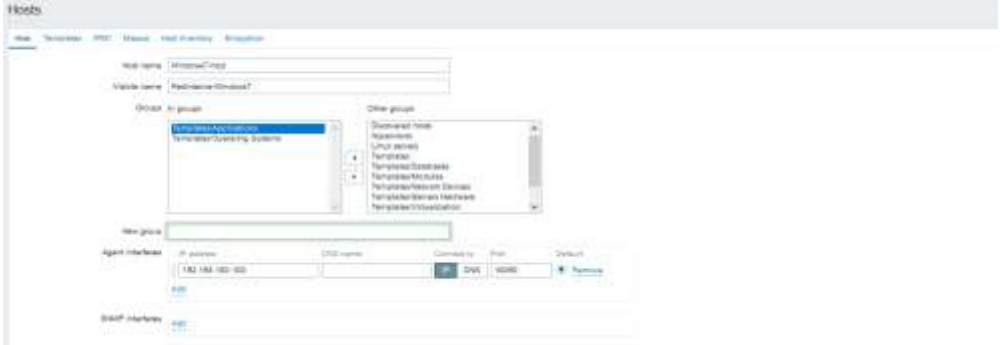
```
#     Example: ServerActive=127.0.0.1:20051,zabbix.domain,
[::1]:30051,::1,[12fc::1]
#
# Mandatory: no
# Default:
# ServerActive=

ServerActive=172.16.0.1

### Option: Hostname
#     Unique, case sensitive hostname.
#     Required for active checks and must match hostname as
configured on the server.
#     Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=

Hostname=Windows7-host
```

3) Instalar servicio

```
C:\Windows\system32>cd c:\zabbix\bin\win64

c:\zabbix\bin\win64>zabbix_agentd.exe -c c:\zabbix\zabbix_agentd.conf --install
zabbix_agentd.exe [1412]: service [Zabbix Agent] installed successfully
zabbix_agentd.exe [1412]: event source [Zabbix Agent] installed successfully
```

4) Agregar hosts al servidor de monitoreo zabbix



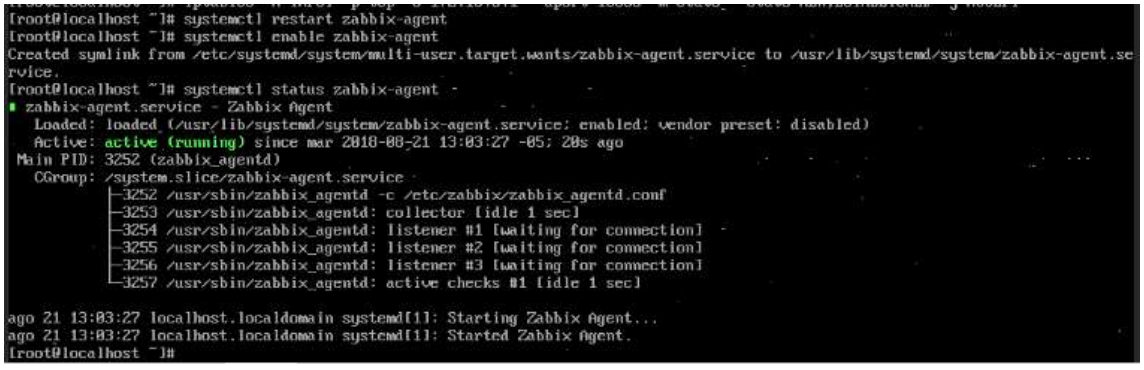


Anexo 19: Manual de instalación de agente zabbix en componente DMZ

1) Descargar e instalar paquete

2) Configurar como agente pasivo

3) Abrir puerto e iniciar servicio



4) Realizar procedimiento similar a **Anexo *18*** para agregar host a servidor zabbix.

Anexo 20: Proceso de sniffeo de redes

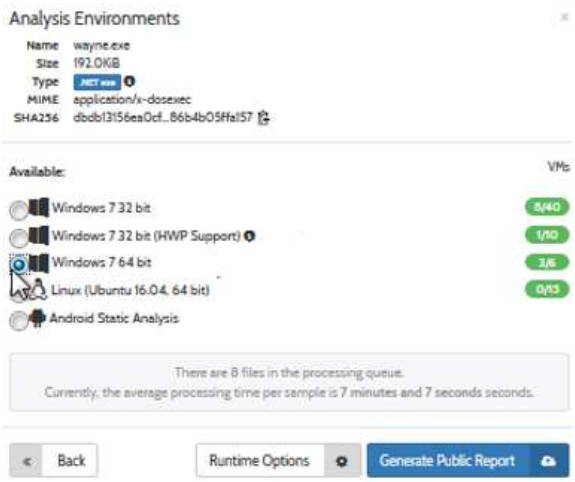
1) Iniciar el proceso de espejo de paquetes, desde una red objetivo hasta otra receptora, usando el demonio «daemonlogger», todo esto en el Shell del hipervisor.

```
root@tesis:~# daemonlogger -i vmbr100 -o vmbr700
[-] Interface set to vmbr100
[-] Log filename set to "daemonlogger.pcap"
[-] Tap output interface set to vmbr700[-] Pidfile configured to "daemonlogger.pid"
[-] Pidpath configured to "/var/run"
[-] Rollover size set to 18446744071562067968 bytes
[-] Rollover time configured for 0 seconds
[-] Pruning behavior set to oldest IN DIRECTORY

-*> DaemonLogger <*-
Version 1.2.1
By Martin Roesch
(C) Copyright 2006-2007 Sourcefire Inc., All rights reserved

sniffing on interface vmbr100
start_sniffing() device vmbr100 network lookup:        vmbr100: no IPv4 address assigned
```

2) Reiniciar servicios de «Moloch» en componente Monitoreo

```
root@monitoreo:~# systemctl restart elasticsearch
root@monitoreo:~# systemctl restart molochcapture
root@monitoreo:~# systemctl restart molochviewer
```

Anexo 21: Elección de entorno para análisis automático de "Wayne.exe" en hybrid-analysis



Fuente: Hybrid-analysis
Elaborado por: Autor

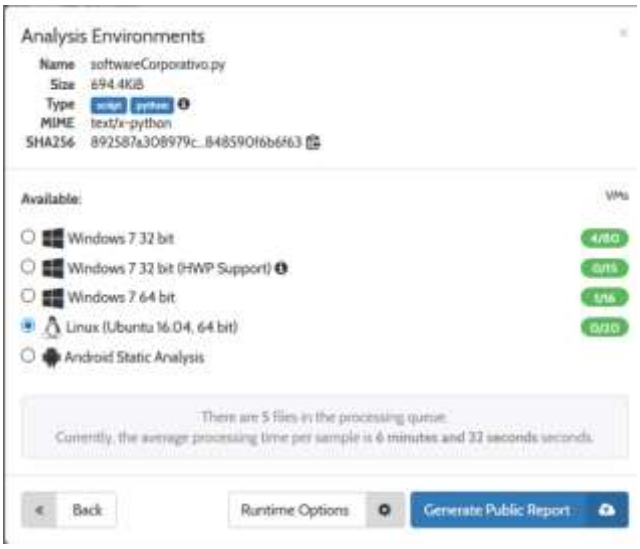
Anexo 22: Clasificación de "wayne.exe" por Hybrid-Analysis

Fuente: Hybrid-analysis
Elaborado por: Autor

Anexo 23: Análisis completo de "wayne.exe" realizado en VirusTotal

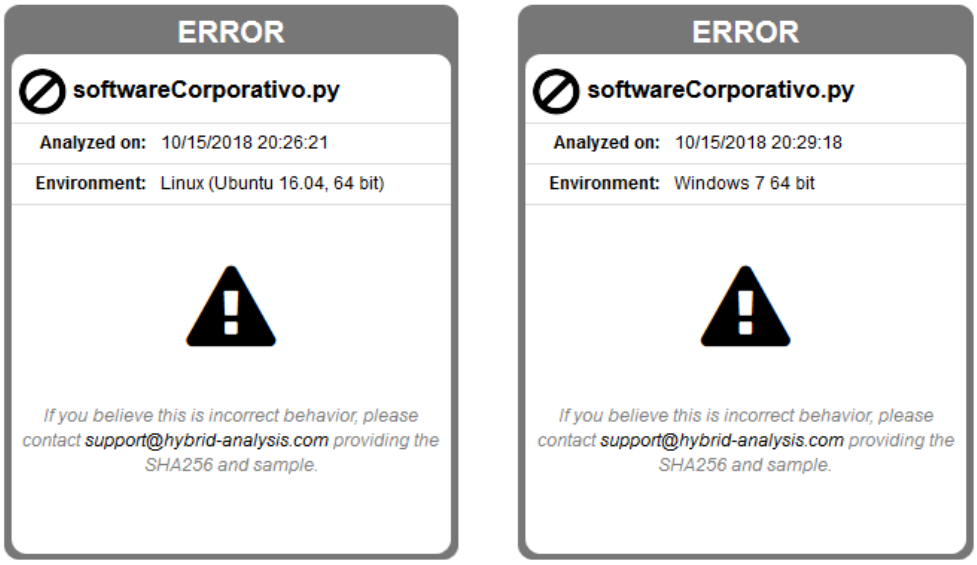
Fuente: VirusTotal
Elaborado por: Autor

Anexo 24: Ambiente de análisis automático para "softwareCorporativo.py"



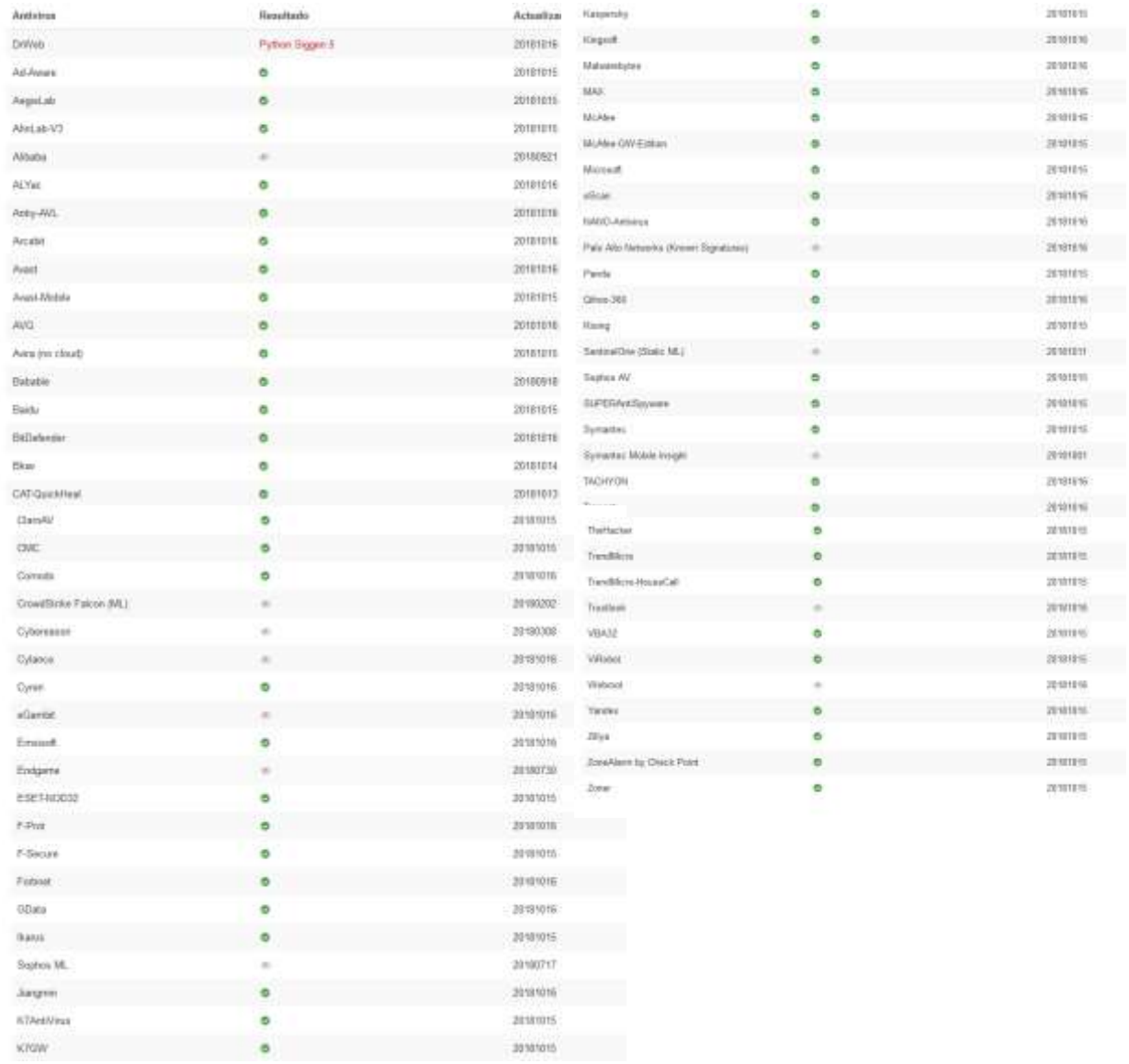
Fuente: Hybrid-Analysis
Elaborado por: Autor

Anexo 25: Error en reporte durante análisis automático "softwareCorporativo.py"



Fuente: Hybrid-Analysis
Elaborado por: Autor

Anexo 26: Escaneo de "softwareCorporativo.py" en VirusTotal



Antivirus	Resultado	Actualizac
DrWeb	Python Skipper.5	20181016
Ad-Aware	✓	20181015
AegisLab	✓	20181015
AhnLab-V3	✓	20181015
Alibaba	✓	20180921
ALYac	✓	20181016
Antiy-AVL	✓	20181016
Arcabit	✓	20181016
Avast	✓	20181016
Avast-Mobile	✓	20181015
AVG	✓	20181016
Avira (no cloud)	✓	20181015
Babable	✓	20180918
Baidu	✓	20181015
BitDefender	✓	20181016
Bkav	✓	20181014
CAT-QuickHeal	✓	20181013
ClamAV	✓	20181015
CMC	✓	20181015
Comodo	✓	20181016
CrowdStrike Falcon (ML)	✓	20180202
Cybereason	✓	20180308
Cylance	✓	20181016
Cyren	✓	20181016
eGambit	✓	20181016
Emsisoft	✓	20181016
Endgame	✓	20180730
ESET-NOD32	✓	20181015
F-Prot	✓	20181016
F-Secure	✓	20181015
Fortinet	✓	20181016
GData	✓	20181016
Ikarus	✓	20181015
Sophos ML	✓	20180717
Jiangmin	✓	20181016
K7AntiVirus	✓	20181015
K7GW	✓	20181015
Kaspersky	✓	20181015
Kingsoft	✓	20181016
Malwarebytes	✓	20181016
MAX	✓	20181016
McAfee	✓	20181016
McAfee-GW-Edition	✓	20181015
Microsoft	✓	20181015
eScan	✓	20181016
NANO-Antivirus	✓	20181016
Palo Alto Networks (Known Signatures)	✓	20181016
Panda	✓	20181015
Qihoo-360	✓	20181016
Rising	✓	20181015
SentinelOne (Static ML)	✓	20181011
Sophos AV	✓	20181016
SUPERAntiSpyware	✓	20181016
Symantec	✓	20181015
Symantec Mobile Insight	✓	20181001
TACHYON	✓	20181016
[illegible]	✓	20181016
TheHacker	✓	20181015
TrendMicro	✓	20181015
TrendMicro-HouseCall	✓	20181015
Trustlook	✓	20181016
VBA32	✓	20181015
ViRobot	✓	20181015
Webroot	✓	20181016
Yandex	✓	20181015
Zillya	✓	20181015
ZoneAlarm by Check Point	✓	20181015
Zoner	✓	20181015

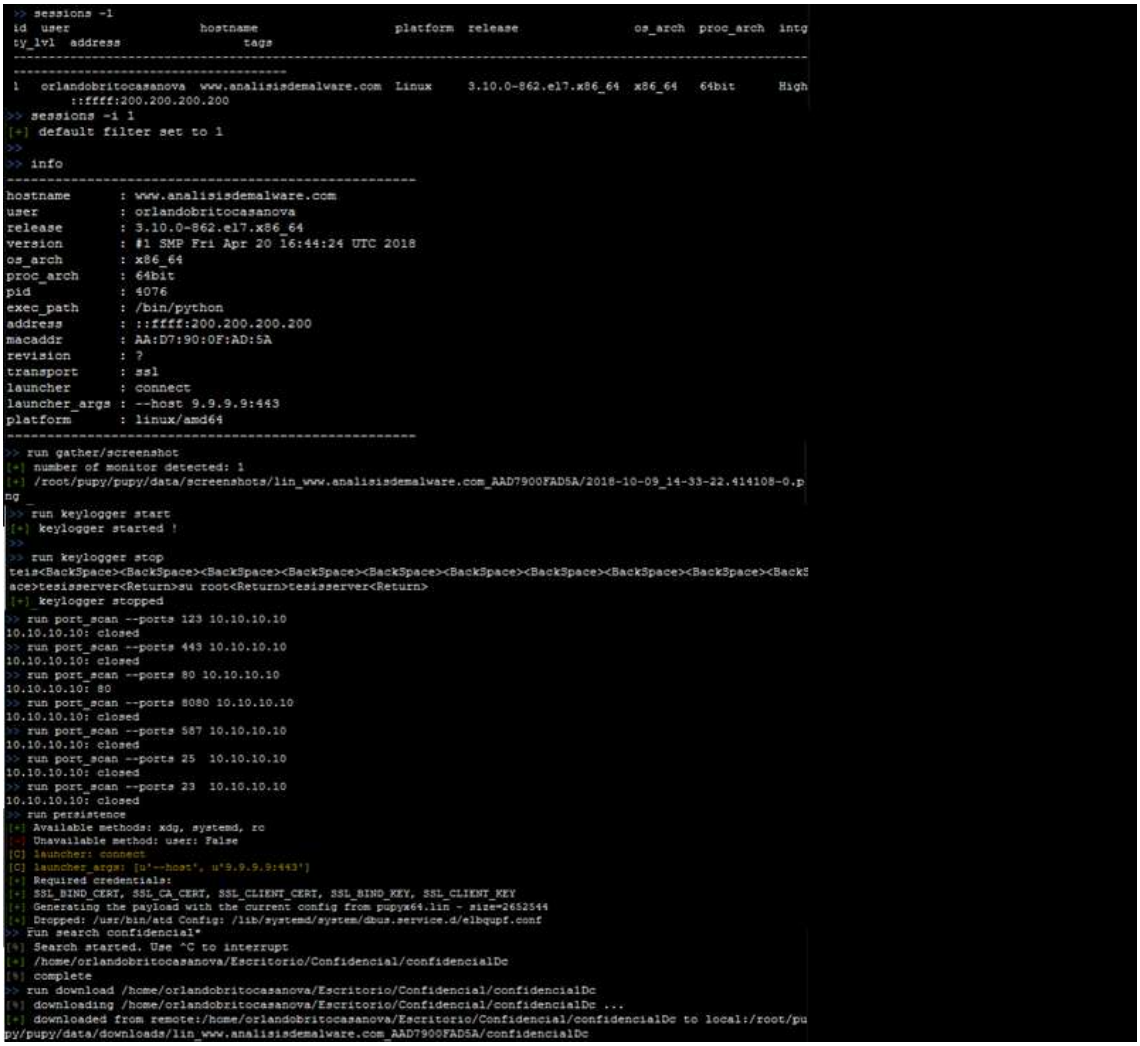
Fuente: VirusTotal
Elaborado por: Autor

Anexo 27: Aislación de logs en servidor INetSim para análisis de "wayne.exe"

```
root@INTERNET-Ubuntu:/var/log/inetsim# sed -n '/2018-09-21 18:28/,/2018-09-22 02:29/p' service.log >2018-09-21_
wayne.txt
root@INTERNET-Ubuntu:/var/log/inetsim# ll -h 2018-09-21_wayne.txt
-rw-r--r-- 1 root root 602K Oct  3 01:27 2018-09-21_wayne.txt
root@INTERNET-Ubuntu:/var/log/inetsim#
```

Fuente: La Investigación
Elaborado por: Autor

Anexo 28: Post-explotacion de componente DMZ empleando "softwareCorporativo.py"



Fuente: La Investigación
Elaborado por: Autor