compAs
Grupo de capacitación e investigación pedagógica

ANÁLISIS DINÁMICO DE MALWARE EN UNA ARQUITECTURA VIRTUAL

Zhuma Mera, Emilio
Brito Casanova, Orlando Jesús

ANÁLISIS DINÁMICO DE MALWARE EN UNA ARQUITECTURA VIRTUAL

Zhuma Mera, Emilio
Brito Casanova, Orlando Jesús

ANÁLISIS DINÁMICO DE MALWARE EN UNA ARQUITECTURA VIRTUAL

compÁs
Grupo de capacitación e investigación pedagógica

Título original: ANÁLISIS DINÁMICO DE MALWARE
EN UNA ARQUITECTURA VIRTUAL

Primera edición: marzo 2020

Publicado por acuerdo con los autores.

Segundo Congreso Internacional de Sociedad y Tecnología
de la información en la Educación Superior
Guayaquil-Ecuador

Editado en Guayaquil - Ecuador

ISBN: 978-9942-33-200-4

compÁs
Grupo de capacitación e investigación pedagógica

Cita.
E. Zhuma, O. Brito (2020) ANÁLISIS DINÁMICO DE MALWARE EN UNA ARQUITECTURA VIRTUAL, Editorial Grupo Compás, Universidad Técnica Estatal de Quevedo. Guayaquil Ecuador, 109 pag

Índice

Prólogo

El libro estudia la viabilidad entornos corporativos virtuales para realización de análisis dinámico de malware, las 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 a su 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, 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.

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 afectar 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; los malwares son código maliciosos diseñados para vulnerar sistemas y causar perjuicios significativos, sea con fines monetarios, activismo e incluso terrorismo. Estos softwares pueden ser obtenidos de diversos orígenes (internet, usb, ingeniería social, vulnerabilidades de software… etc.), y poseer uno o más de los siguientes componentes: Ocultador, forma de permanecer indetectables; Replicador, manera de propagarse; Bomba, ejecución de ataque.

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.; Dinámico, implica la ejecución del código y monitoreo de su comportamiento en el sistema. Estás técnicas tienen como objetivos la obtención de firmas[1], cuales puedan ser usadas por antivirus para identificación.

El análisis dinámico debe de realizarse en un laboratorio con ambiente controlado, debido a las dificultades

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

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[2], 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 en el cómputo en la nube.

El presente estudio expone las capacidades brindadas por tecnologías de virtualización para el desarrollo de análisis dinámico de malware tanto en sistemas independientes, como en una completa topología de red de común uso entre empresas de medianas o sucursales de grandes corporaciones.

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

Capítulo 1

Presentación de la investigación

El malware (software malicioso) está diseñado para explotar vulnerabilidades existentes en las redes o sistemas informáticos con objetivos no éticos, afectando negativamente el funcionamiento de los mismos. Ningún tipo de dispositivo o red se encuentran exentos completamente de una infección[3], tanto en ambientes domésticos, corporativos o industriales puede originarse situaciones de alto riesgo con impactos significativos. 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.

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

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

[3] Estado de contraer un software malicioso ya activo en el sistema.

Cada uno de los softwares maliciosos expuestos poseen una o más de los siguientes tres componentes definidos según el consultor de ciberseguridad[4] Munir Njenga como:

- Ocultador: Esta característica o función habilita al malware permanecer indetectable incluso por los programas antimalwares[5].
- 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.

Los malware pueden ser dirigidos de manera general, así como creados por ciberterroristas[6] destinados a afectar una determinada organización u empresa, siendo este motivo gran preocupación dentro del mundo empresarial. Por ello, ESET realizó una encuesta titulada *Security Report Latinoamética 2017*, con una población de más de 4 mil ejecutivos y profesionales IT de diversos países Sur y Centro Americanos, denotando como principal preocupación la infección por software malicioso con un 56% debido "*al grado de sofisticación que tiene el malware y el retorno económico que genera; y que sigue en aumento*" [3].

Según [3], una de cada dos empresas latinoamericanas participantes en su estudio presentaron inconvenientes con algún tipo de malware, esto equivale al 49% de los encuestados, también establece la importancia del estudio por separado de Ransomwares por las repercusiones producidas en las organizaciones en la actualidad, con un

[4] Protección de información, estudio y respuesta de amenazas que involucren redes y sistemas.
[5] Software de monitorización de sistemas que prevé infecciones.
[6] Persona o grupo de personas con fines de infundir el terror en medios informáticos

16% ocupa el segundo lugar de los incidentes de seguridad en empresas latinoamericanas.

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*" [4]. 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 [4] 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 [5] con el fin de aclarar conceptos.

- Análisis estático básico.- Estudia el código del malware empleando un escaneo con antivirus, realizando hashing[7] o detección del empaquetado, así como analizando la estructura del ejecutable propiedad del malware.
- Análisis estático avanzado.- Emplea herramientas adicionales, analizando Strings[8] y librerías vinculadas usando desensambladores[9].
- 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[10] el malware, analizando registros y haciendo un análisis íntegro de todo el sistema de estudio.

Existe la posibilidad de realizar un análisis completamente automatizado, empleando herramientas tanto disponibles comercialmente así como gratuitas, cuales evalúan los efectos del malware simulando su ejecución en un sistema real. El instituto SANS 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*" [6], pero no dejan de ser herramientas

[7] Transformación del código en una cadena de caracteres de longitud fija.
[8] Secuencia de caracteres imprimibles
[9] Traduce lenguaje de máquina a lenguaje ensamblador
[10] Ejecutar el programa siguiendo todas sus acciones

poderosas que pueden usarse como primer paso de un análisis profundo.

Los entornos virtuales empleando tecnología VMWare[11] 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?*" [7].

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*" [8]. 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.

El crecimiento de la cantidad de malware liberados indica que cada vez existen mayor número de desarrolladores,

[11] Líder en infraestructura de nube y tecnologías de virtualización

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, sino se desarrollan también tomando en cuenta los objetivos de la seguridad informática y de redes. El desarrollo de nuevos dispositivos inteligentes "*Smarts*" y su masificación los convierten en blancos perfectos; en caso de no tomar las medidas necesarias para su protección, se podría realizar ataques de todo tipo proporcionados por los malware, como el robo de claves bancarias, suplantación web, robos de datos de la tarjeta de crédito y la vulneración de privacidad con fines extorsivos.

Otros de los conceptos futuristas que están siendo aplicados en el presente son el Internet de las Cosas "*IoT*"[12], el cual ha sido fuertemente vulnerado, debido a varios factores, destacando la limitada cantidad de procesamiento que poseen dichos dispositivos en que aplicar técnicas de seguridad informática ralentizaría sus operaciones. Se estima que para el 2020 existan veinte billones de dispositivos IoTs conectados a la red, resultando objetivos de códigos maliciosos con el fin de crear grandes Botnets[13] y realizar ataques DDOS en extremos difíciles de mitigar. Además con la propagación de los *Ransomwares*, han surgido variantes aplicadas para los dispositivos mencionados, son conocidas como RoT "Ransomware de las Cosas" e involucra el bloqueo de los dispositivos para pedir el pago de un rescate. Las bondades y posibilidades de estas redes son conocidas por el público en general, en donde según ESET Latan[14] "*El 81% de los usuarios opina que la llegada de internet de las cosas*

[12] Internet de las Cosas.- sistema de dispositivos interrelacionados y conectados a internet
[13] Diversos equipos "zombies" en espera a código para realizar ataques en conjunto.
[14] Empresa desarrolladora de antivirus y soluciones de seguridad.

brinda más comodidad a la vida cotidiana" [9] pero también se ve 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*" [9].

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, son aquellos que "*pueden transformarse en función de su capacidad de traducir, editar y reescribir su propio código*" [10]; 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 análisis.

Debido a la sofisticación y complejidad de los malware de última generación, así como al incremento del desarrollo de nuevos software maliciosos, es imprescindible el uso de diversas herramientas y técnicas para su estudio y análisis con el fin de proporcionar una respuesta ágil. Los incidentes de seguridad relacionados con malware han ascendido respecto a años anteriores, según lo indicado por el Instituto SANS [3], esto debido a la creciente cantidad de código maliciosos desarrollados y liberados en la actualidad, nuevos

métodos de propagación y mayores ganancias monetarias obtenidas por los desarrolladores.

Los malwares tienen efectos desbastadores en empresas u organizaciones, provocando grandes pérdidas económicas y de reputación, influyendo negativamente en la percepción de confiabilidad desde sus clientes. Las redes corporativas suelen contar con diversos elementos, dependiendo del tamaño de la empresa, cuáles pueden ser vulnerados o de alguna forma infectados con código maliciosos afectando la operatividad de toda una red, causando: ralentización, pérdidas de paquetes, denegación de servicios e inclusive robo de secretos empresariales.

El análisis dinámico[15] de malware destinado a corporaciones, debe de realizarse en ambientes controlados lo más exactamente parecidos a entornos reales involucrado, esto conlleva el uso de equipos de networking, firewalls, servidores y distintos host finales para evaluar el comportamiento real de software malicioso y sus objetivos. La creación de un laboratorio físico implica la inversión de una enorme cantidad de dinero, factible para grandes empresas de investigación y universidades, pero, totalmente inconcebible para investigadores independientes; quienes globalmente también realizan contribuciones importantes con respecto al análisis de comportamiento y detección de malwares.

La virtualización es la opción más usada por los investigadores, Actualmente los programas de virtualización abarcan mayores funcionalidades, como la realización de snapshots[16], el completo aislamiento del sistema, así como la interconexión virtual de equipos simulando redes, para

[15] Instantánea (análogo a foto) de un sistema en un momento exacto, que pueda analizarse.
[16] Análisis de malware que involucre la ejecución real del espécimen para monitorear su comportamiento.

obtener una percepción de su funcionamiento como conjunto. Los softwares de virtualización tendrán una mayor importancia futura, por lo que es imprescindible el estudio de las capacidades y limitaciones actuales con respecto a simulación de entornos de red completos para realizar un correcto análisis dinámico.

Aplicación de metodología de malware para el análisis de la amenaza avanzada persistente (APT) "Poison Ivy".

Gaviria [11] 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[17] y la implementación de laboratorio virtual correctamente aislado, como parte de la metodología aplicada.

Vulnerabilidades y seguridad en redes TCP/IP.

Mancheno y Robles en [12], 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.

[17] Herramienta de acceso remoto

Practical Malware Analysis

Sikorski y Honing en [4], 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.

Análisis digital de una infección de malware en sistemas Windows

Arce [13] describe el análisis de situación contemporánea a su año sobre el estado de malware y estadísticas de distintas organizaciones, poniendo en perspectivas la significación 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».

Análisis dinámico de malware en entornos controlados.

Suárez [14] 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.

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

Latorre [15] 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.

Metodología para el análisis de malware en un ambiente controlado

Jumbo en [16], 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.

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*" [17]. 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[18], está conformada por una o más "Redes de Área Co0rporativas" (CAN), partes aisladas y protegidas de una intranet[19] 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.

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 [18], que deben ser consideradas al momento de diseñar una arquitectura de red, expuestos en los siguientes puntos.

- **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. Al dividir el tráfico en paquetes, pueden ser dirigidos al destino a través de distintas rutas (enlanches físicos), reduciendo la posibilidad de errores.

- **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

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

con protocolos estandarizados y tomando en cuenta el crecimiento posterior de la organización.

- **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[20] 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.

Topología 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

[20] Suma de retardos temporales dentro de una red

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. [19]

- **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, 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. [19]

- **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. [19]

- **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. [19]

- **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. Dado que existen varias estructuras de bus, cada una debe de incorporar sus terminadores y elementos asociados, así como los elementos de enlace. [19]

- **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

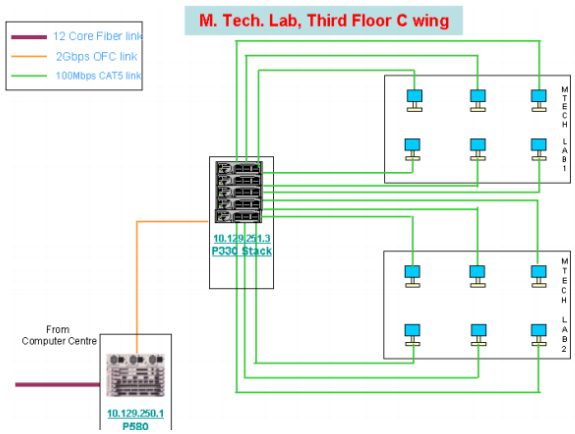
principal y control de la red, este queda implícito en cada nodo. Durante la ampliación o reducción de la red, el funcionamiento se ve obstruido, un fallo en la línea provoca la caída de la red. También se la conoce como red "testigo" o "Token ring". Posee una relación coste-modularidad bastante positiva, 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. [19]

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. [20]

- 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"

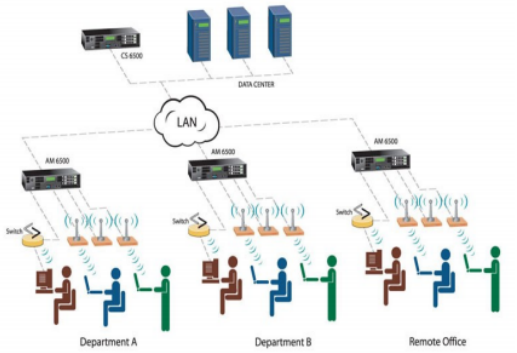


Fuente: Sridhar Iyer

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.

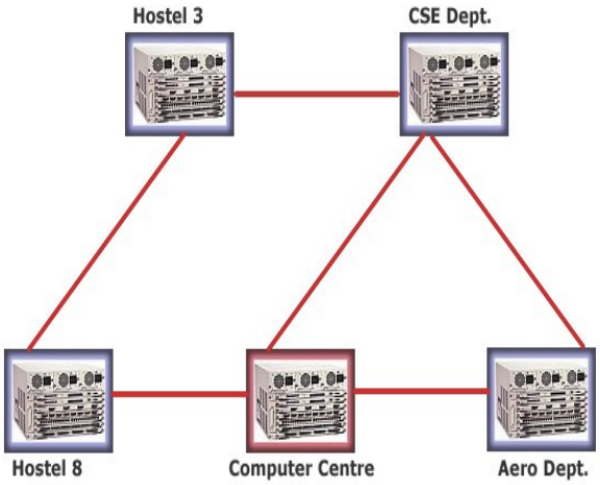
Ilustración 2: Representación de nivel "mili"



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.

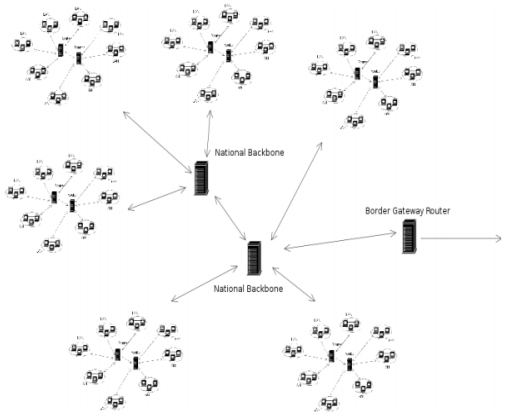
Ilustración 3: Representación de nivel "típico"



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

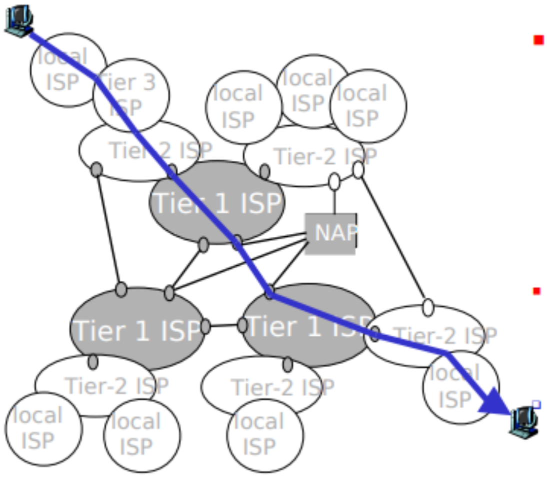
Ilustración 4: Representación de nivel "Kilo"



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.

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, guest*)" [21], 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. [22]

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. [19]

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.

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" [23].

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. [22]

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. [22]

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. [22]

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.

Softwares de virtualización populares

KVM

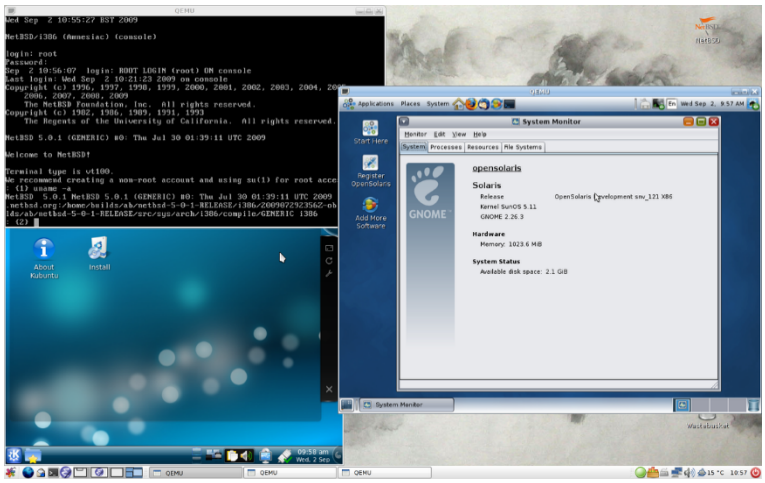
(Kernel based Virtual Machine). Basada en GNU/Linux y desarrollada por la empresa Qumranet, Permite la virtualización sobre hardware X86 y viene incluido por defecto a partir del Kernel 2.6.20 de Linux. KVM realiza una virtualización completa, a diferencia de otros sistemas que emulan el procesador (Virtual Box, VMWare), dando mucha usabilidad y flexibilidad, pero no aprovecha bien los recursos del servidor, a continuación se exponen ciertas características [24]

- 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

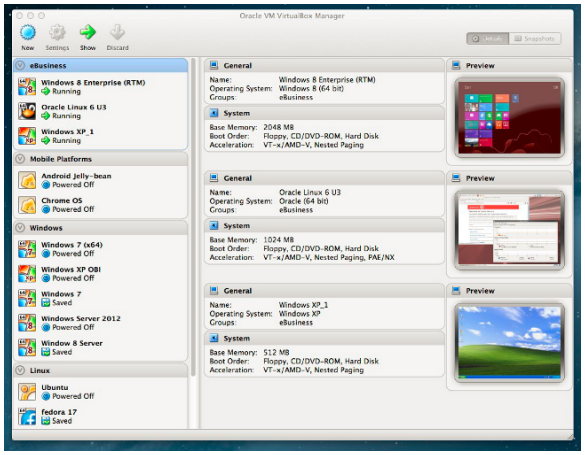
VirtualBox Oracle VM

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

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. [25]

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. [24]

Ilustración 8: Creación de nueva máquina virtual VMWare

Fuente: adictosaltrabajo.com
Elaborado por: adictosaltrabajo.com

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. [24]

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. [24]

Ilustración 9: Logo de XEN Project

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

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. [24]

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. [26]

Ilustración 10: Entorno de Virtual PC

Fuente: pcmag.com
Elaborado por: pcmag.com

Clasificación de Malware

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: [27]

- 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

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 alteral 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. [27]

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. [27]

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. [27]

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. [27]

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. [27]

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. [27]

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). [27]

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. [27]

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. [27]

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. [27]

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). [27]

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. [27]

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. [27]

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. [27]

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. [27]

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. [27]

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. [27]

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. [27]

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. [27]

Generalidades de Análisis de Malware

Existen 2 técnicas para análisis de malware cubiertas en este proyecto: Técnica de análisis estático o de código; Técnica de análisis dinámico o de comportamiento.

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. [15]

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. [15]

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)

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. [15]

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. [15]

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. [15]

Localización

El presente proyecto se centra en el estudio de los principales elementos de una red corporativa típica, enfocado en medianas o pequeñas empresas, así como de sucursales de grandes corporaciones. Suelen estar localizadas en ciudades de relevancia económica para la región, contando con diversas ubicaciones; generalmente zonas céntricas con facilidad de recursos (transporte, tecnología), tanto como en locaciones industriales. Es común el almacenamiento de componentes tales como: routers, servidores (dns, correos, páginas web) o firewall; dentro del área de administración de TIC's contando con un ambiente propicio para su preservación dentro de las instalaciones de la empresa. Los elementos finales son ubicados en diversos departamentos donde sean requeridos (recursos humanos, marketing…etc), e interconectados mediante switches.

La investigación está enfocada en la creación de entornos virtuales y su interconexión lógica para simular un ambiente de red corporativo. Al crear un laboratorio virtual de análisis, se propicia un mayor control sobre diversos aspectos de las redes, como la posibilidad de regresar a estados previos después de la ejecución de malware, facilitando la aplicación de diversas técnicas. Su ubicación corresponde a la máquina real en donde se aloje al software de simulación. 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.

Desde los resultados obtenidos

La elección de una topología de red empresarial juega un rol fundamental para el desarrollo en un laboratorio de análisis de malware, y la complejidad depende del tamaño de su infraestructura y los servicios brindados a la organización. Una topología de seguridad perimetral empleando una zona desmilitarizada, red interna, firewall- router e internet, es de amplio uso entre empresas medianas, pequeñas o sucursales de una gran corporación, con posibilidades de abstracción de cada uno de sus componentes en elementos básicos, conservando la funcionalidad y operatividad de una red completa.

Breve análisis de topologías empresariales.

La D.R.A.E[21] define como empresa a la "*unidad de organización dedicada a actividades industriales, mercantiles o de prestación de servicios con fines lucrativos*" [29], 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

[21] Diccionario de la Real Academia Española

importancia de la incorporación de nuevo conocimiento al sector productivo [30].

El desarrollo en las tecnologías computacionales y en las telecomunicaciones en general, se aplica en la operatividad de las organizaciones, siendo pilares 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" [31].

Elección de topología

Si bien el diseño topológico físico de una red empresarial depende del tamaño de la corporación así como los servicios que su infraestructura preste, se debe de tomar a consideración los recursos necesarios para su completa virtualización; a mayor elementos virtualizados, más capacidades computacionales será requerida. Con el objetivo de virtualizar una red completa de una organización real 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 una unidad elemental y la implementación de políticas de seguridad y configuraciones análogos a la realidad. Se adoptó 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 optó por la utilización de una modesta topología de seguridad perimetral de amplio uso empleando una DMZ con un cortafuego en trípode, siendo una abstracción de una red empresarial a nivel mili, según la categorización por tamaño de Sridhar Iyer [20], adicionando una red de monitoreo.

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

Abstracción de componentes y elección de Sistemas Operativos

Siguiendo la estructura especificada, se buscó abstraer la funcionalidad de cada componente, representándolos en

una única entidad. No es necesario la creación de una topología de gran tamaño debido a los fines de la actual investigación, se necesita representar una arquitectura funcional, que pueda ser utilizada para la realización de análisis dinámico. No obstante, si se requiere un estudio de los componentes en forma individual, es factible la utilización de una mayor cantidad de elementos, siempre y cuando se cuente con los recursos necesarios.

Componente Red Interna.

Correspondes 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 los 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 algunos 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, con un total de 36,22% del mercado. Esto se complementa con las estadísticas reflejadas en «netmarketshare.com» , 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 decidió 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.

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*" [32], puede estar conformada por 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 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, 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 optó 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.

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 dichas y otros complementos (DHCP, DNS, NAT, etc). La elección de un elemento representativo a virtualizar se basa en componentes mayormente usados en las organizaciones, por ello se toma a consideración el ranking expuesto hasta junio de 2018 por «itcentralstation.com», 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 optó por 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).

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 [33], muy a menudo el código estudiado, intenta el establecimiento de conexión con equipos remotos a través de internet, en 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.

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 eligió INetSim (para plataformas Linux) como herramienta para generar respuestas falsas de varios protocolos usuales de internet, implementado en una máquina con sistema operativo Ubuntu.

Conmutación con RAT PUPY

La herramienta de acceso remoto PUPY es una contribución desarrollada y distribuida en GITHUB, si bien posee fines tales como en 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.

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.

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 [34], [35], [36].

El componente "Monitoreo" es abstraído de servidores y equipos focalizados en 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 optó por la implementación de Moloch como sniffer principal y Zabbix como herramienta de monitoreo interno, implementados en S.O Ubuntu 18.04.1, ambas herramientas constan de su respectiva web-GUI[22], la cual puede ser accedida por un computador en red con el servidor de virtualización y conexión real a internet.

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

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

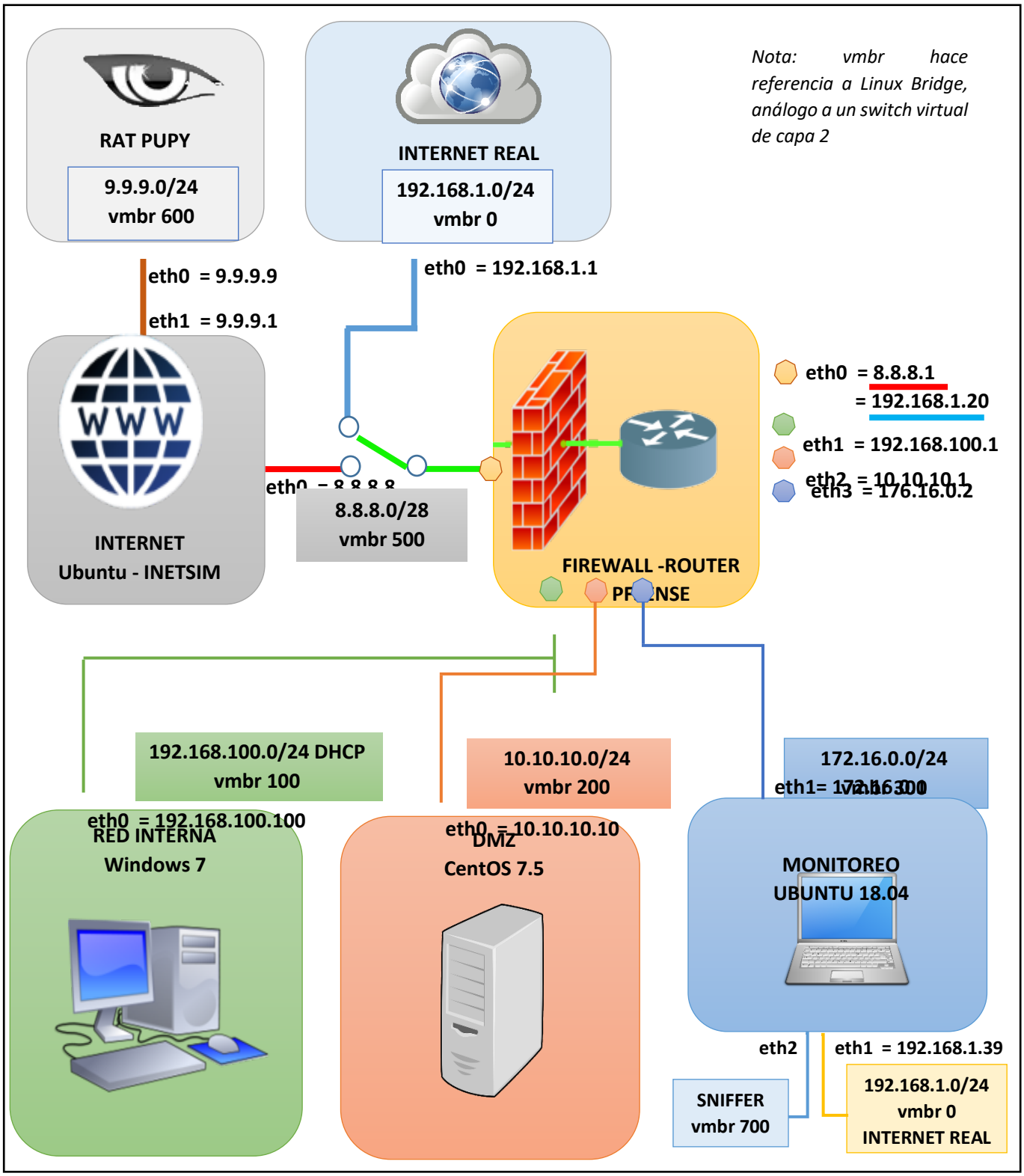
[22] Administración y control mediante página web contenida en servidor de la herramienta

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

Diseño y topología de red empresarial

Ilustración 11: Topología lógica de red empresarial a implementar



El establecimiento de un entorno aislado juega un rol importante para el desarrollo seguro de análisis dinámico, el cual puede realizarse desde un solo computador, hasta el estudio de una topología de red completa real 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.

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" [37], 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.

Se resume las características de virtualización escogidas según las directrices anteriores para la definición de una plataforma de virtualización, según una 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).

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 por 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. [37]
Arquitectura	**Hipervisor**	Permite que varios S.O. se ejecuten simultáneamente en

	un solo host físico, así como también proporciona abstracción de hardware al SO huésped (Guest OS) y multiplexa de manera eficiente los recursos de hardware subyacentes. [37]

Fuente: La investigación
Elaborado por: Autor

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» (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.

Se opta por elección de Proxmox VE en su versión 5.2 como plataforma de virtualización, al contar este 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.

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.

Tabla de requerimiento mínimo y recomendable para Proxmox.

Información obtenida en la wiki oficial pve.proxmox.com [38].

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

Tabla de requerimientos mínimos por sistema operativo.

Con lo estipulado durante el desarrollo de la etapa 1 del presente proyecto, se expone tablas de requerimientos mínimos por sistema operativo a implementar para definir la distribución de recursos.

Requerimientos mínimos por sistema operativo

Requerimiento	***Windows 7*** *[39]*	***Ubuntu 14.04 (cli)*** *[40]*	***CentOS 7.5*** *[41]*	***PFSENSE*** *[42]*
CPU	1 GHz	300 MHz	300 GHz	500 MHz
RAM	1 GB	225 Mb	1 GB	512 Mb
Disco Duro	20 GB – 64 bits	1,5 GB	2 GB	1 GB
Tarjeta de Red	-	-	-	Mínimo 2

Fuente: La investigación
Elaborado por: Autor

Tabla de recursos disponibles y su distribución entre los distintos componentes

El rendimiento de la topología ejecutada simultáneamente depende de las capacidades contadas

respecto a recursos hardware del servidor físico en donde se implementa, 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 permitiendo una mejor realización de la investigación propiamente dicha. La muestra la definición de los recursos para cada componente así como las características hardware del servidor físico.

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 – 1 GB de swap	1
Pfsense 5.2	2 núcleos	32 GB	1 – 3 GB	3

Fuente: La investigación
Elaborado por: Autor

Creación e instalación de Máquinas Virtuales.

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 estos junto con memorias

USB los principales medios de instalación. 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.

Fuentes de Imágenes ISO

	Fuente	***Descripción***
PROXMOX 5.2	Proxmox.com[23]	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[24]	Al ser un sistema operativo bajo licencia comercial, se optó por la descarga de una prueba de 90 días, tiempo suficiente para el desarrollo de la investigación.
CentOS 7.5	Centos.org[25]	Al ser software libre y gratuito, su descarga se simplifica al ingreso de la página oficial y en la elección del .iso conveniente, se optó por el modo "Everything ISO", cual

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

		proporciona todos los recursos en un solo archivo (8.8 GB)
Pfsense 2.4.3	Pfsense.org[26]	Es de código abierto por lo que su obtención es totalmente gratuita, pero se debe especificar la versión, medio de instalación y arquitectura de CPU

Fuente: La investigación
Elaborado por: Autor

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 se debe de preparar el equipo físico a implementarse, los recursos debe de ser los suficientes para permitir la creación y ejecución simultánea de varias máquinas virtuales; además, como indica [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, se debe de considerar los programas usados para conversión a un USB booteable[27] (no funciona con UNetbootin or

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

Rufus), como es indicado en [45], se usó "etcher" en el flasheo del dispositivo.

- El proceso de instalación es gráfico e intuitivo, pasando desde el formato del disco (se usó todo el espacio disponible) hasta la configuración regional y direccionamiento IP. Se debe de tener precaución con la ip configurada, debido a que mediante esta, se lleva a cabo el acceso a la WEB GUI de Proxmox mediante el protocolo HTTPS por defecto en el 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). Si se tiene acceso a la web, dentro de nuestro nodo, en la sección '/System/Network' se posibilita la edición de vmbr0.

Creación de Bridges

Un puente (bridge) es una abstracción de un switch de capa 2 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 que se pueda crear 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, se debe 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 nuestro nodo a

configurar, se procede a la búsqueda de la sección 'System/Network', que muestra todas nuestras interfaces disponible, para posteriormente dentro de menú disponible escoger 'Create – Linux Brige'. Para efectos de aislación de red, únicamente se configura el nombre del puente.

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 12: 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

Elección de tecnologías de virtualización según componentes

Proxmox virtualiza elementos usando dos tecnologías, cuales poseen cualidades diferentes que las hace indicadas para cierto tipo de máquina virtual según los requerimiento. Estas tecnologías son: LXC (usado en la implementación de containers[28] CT), permite la ejecución de un sistema operativo completo dentro del núcleo del hipervisor, esto imposibilita 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.

[28]Alternativa ligera a virtualización completa

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 decidió en su utilización para el levantamiento del servicio INetSim (emulación de Internet), servidor Pupy (herramienta de acceso remota), e implementación de un servidor de monitoreo con los servicios Moloch y Zabbix.
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 lo son Windows 7 y Pfsense (FreeBSD); no obstante se decidió su implementación en la creación de la red DMZ al brindar mayor aislamiento e independencia del sistema hipervisor.

Fuente: La investigación
Elaborado por: Autor

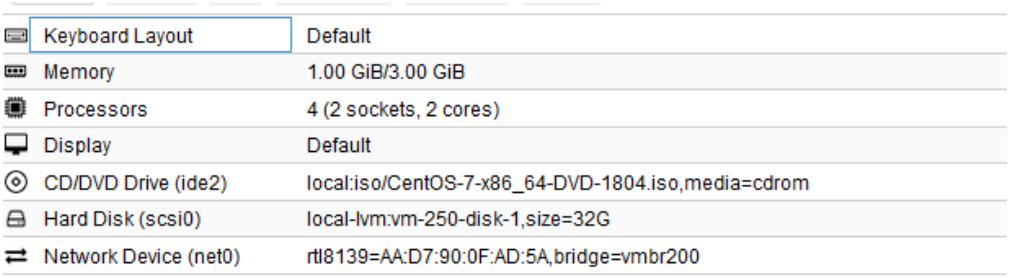
El proceso de creación y obtención de los recursos de instalación difiere entre estos dos sistemas de virtualización; VM trabaja directamente con las .iso descargadas de diferentes fuentes, estas se suben directamente al storage local de proxmox; en cuanto se refiera a CT, es necesario la obtención de templates LXC, los mismos que pueden ser obtenidos desde el propio proxmox y no requieren del proceso de instalación del sistema operativo.

Ilustración 13: 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

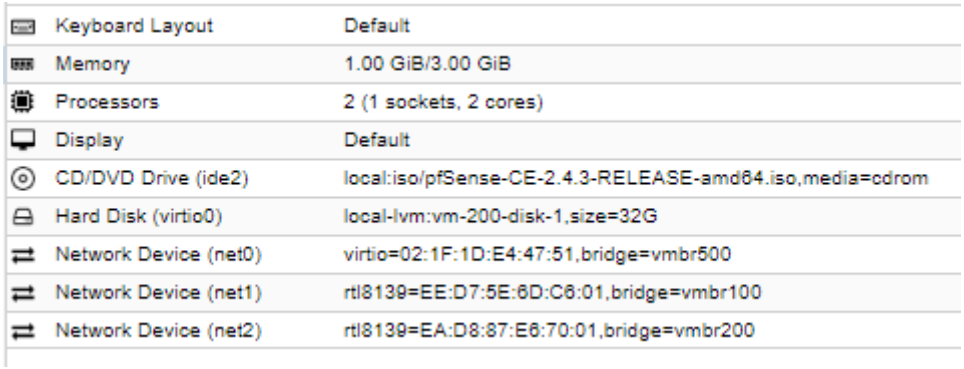
Ilustración 14: Hardware implementado para elemento VM CentOS



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

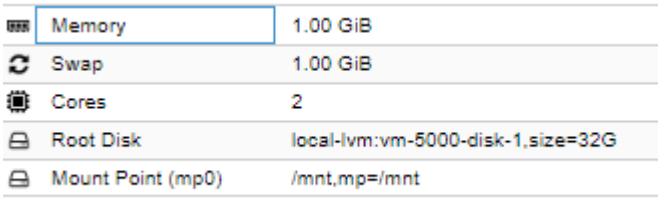
Ilustración 15: Hardware implementado para elemento VM PFsense



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

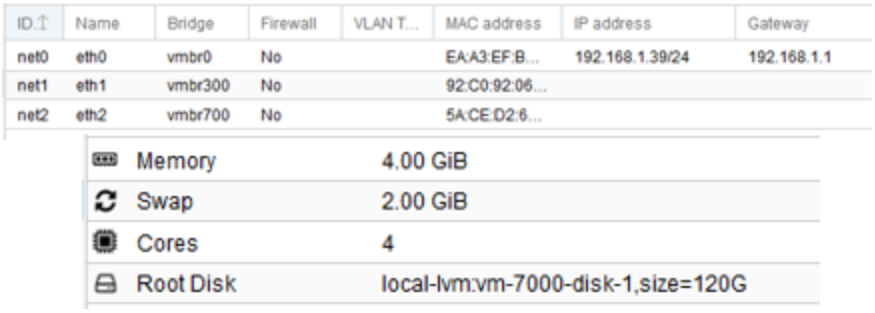
Ilustración 16: Recursos implementados en CT Internet – Ubuntu



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 17: 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

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, se procede a realizar la instalación de los elementos que así lo requieran, para ello se deben de tener a consideración los recursos definidos para cada máquina virtual.

Breve descripción de instalación para los S.O requeridos

Elemento	***Sistema de virtualización***	***Descripción de Instalación***
Windows 7	VM	Se realizó una instalación típica de una versión de prueba (90 días) al no contar con licencia de activación.
CentOS 7.5	VM	Se siguió el procedimiento definido por el asistente de

		instalación gráfica en 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 el particionamiento del disco.
Ubuntu 14.04	CT	No necesitó de instalación alguna al provenir de un template obtenido mediante repositorios libres de Proxmox.

Fuente: La investigación
Elaborado por: Autor

Configuraciones e implementación de red empresarial.

Configuración de INETSIM (Componente Internet)

Antes de proceder a la descarga e instalación de la suite INETSIM para Ubuntu se debe de preparar el entorno; establecer vmbr0 como puente, para de esta manera poseer acceso a internet; se necesita de la instalación de los requerimientos como prerrequisitos para el correcto funcionamiento del software en 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, se debe de actualizar la lista de repositorios, este se lo realiza agregando la línea ***'deb http://www.inetsim.org/debian /binary'*** en el archivo ***'/etc/apt/sources.list'*** y descarga 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'*** se procede a 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'*** en 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'***.

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 potente código malicioso con la 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.

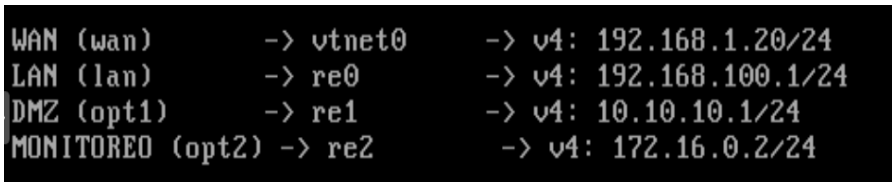
Ilustración 18: Directorio /root/pupy/pupy

Fuente: VirusTotal.com
Elaborado por: Autor

Configuración de PFSENSE (Componente Firewall – Router)

Pfsense cuenta con una potente interfaz web de configuración, la cual puede accederse mediante la dirección IP configurada para su interfaz LAN (eth1). Las configuraciones iniciales pueden 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 se procede a configurar el direccionamiento IP por interfaz.

Ilustración 19: Direccionamiento IP y asignación de



interfaz pfsense
Fuente: La investigación
Elaborado por: Autor

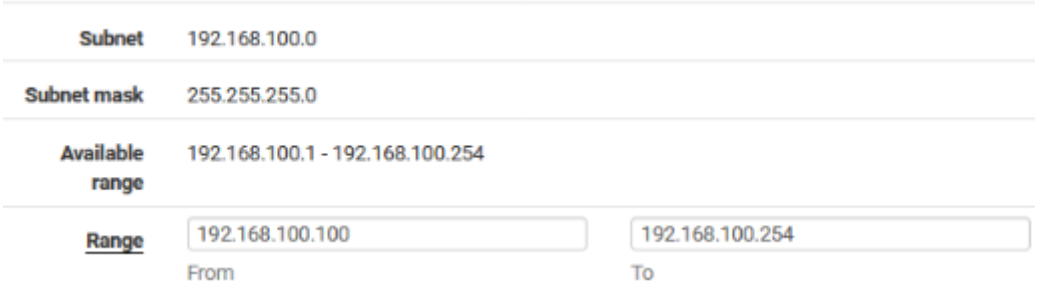
El acceso a la WEB GUI se lo realiza usando la VM Windows 7 ubicada en la componente LAN y con direccionamiento IP estático inicialmente con el Gateway correspondiente la interfaz LAN de pfsense. Mediante https y la dirección

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 se recomienda su cambio) para el usuario y contraseña respectivamente.

La componente Firewall-Router se encarga de cumplir varias funciones, como, servidor DHCP para la 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 se habilita el servicio DHCP con los parámetros indicado, 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 20: 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, se emplea el servido DNS Resolver, cuya configuración se realiza en 'Services/DNS Resolver/General settings', lo cual al recibir una petición dns (puerto 53) para los dominios determinados, devolverá la dirección ip correspondiente.

Ilustración 21: Configuración de DNS resolver, pfsense

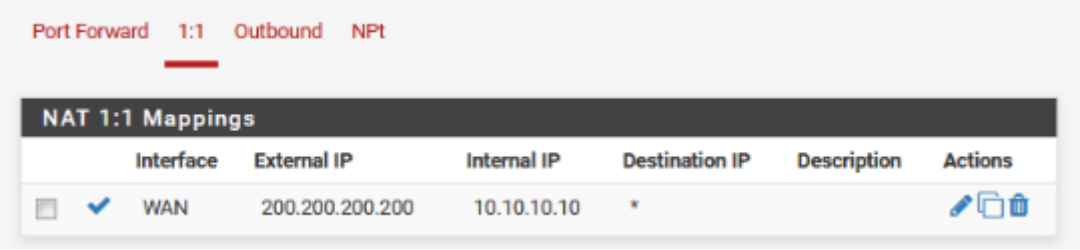
Host Overrides

Host	Parent domain of host	IP to return for host	Description	Actions
	www.analisisdemalware.com	10.10.10.10		
www	analisisdemalware.com	10.10.10.10		

Fuente: La investigación
Elaborado por: Autor

Se usa NAT para traducir direcciones ip o puertos, es una implementación obligatoria 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 usó la funcionalidad 1:1, con la cual se asigna una dirección IP pública específica a dicho host (configuración realizada en 'Firewall/NAT/1:1'; por otra parte se usó un nateo manual outbound para permitir la salida de equipos conectado en la red LAN empleando la dirección IP del puerto WAN.

Ilustración 22: Nateo 1:1 para componente DMZ



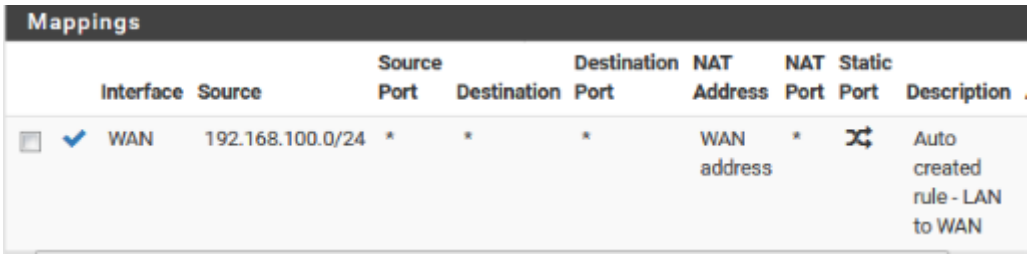
Port Forward | 1:1 | Outbound | NPt

NAT 1:1 Mappings

	Interface	External IP	Internal IP	Destination IP	Description	Actions
	WAN	200.200.200.200	10.10.10.10	*		

Fuente: La investigación
Elaborado por: Autor

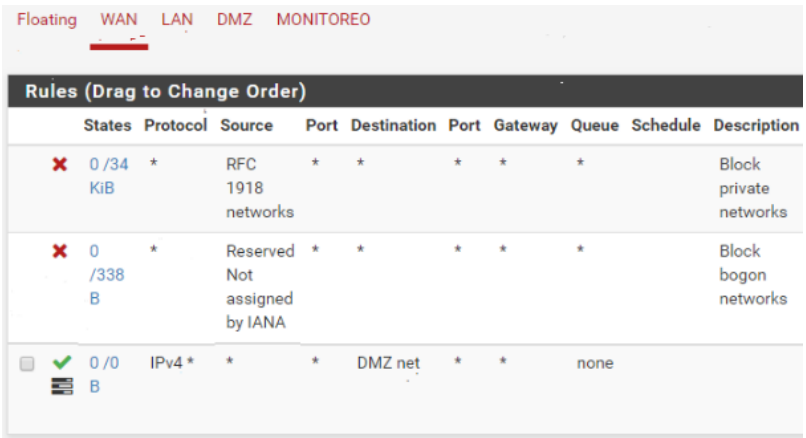
Ilustración 23: Nateo manual Outbound para compoente LAN



Fuente: La investigación
Elaborado por: Autor

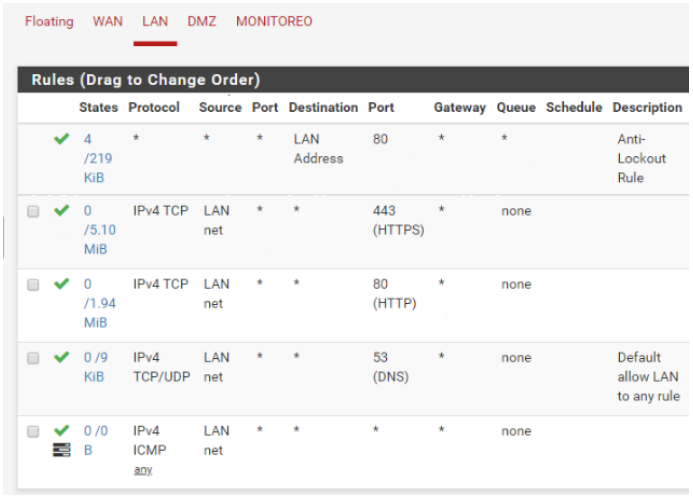
Con lo correspondiente al Firewall, se realizó una configuración implementando políticas de seguridad estándares para redes internar y zonas desmilitarizadas siguiendo lo recomendado en [48], la configuración se realiza en "Firewall/rules" y se diferencia para cada interfaz.

Ilustración 24: Reglas para interfaz WAN, pfsense



Fuente: La investigación
Elaborado por: Autor

Ilustración 25: Reglas para interfaz LAN, pfsense



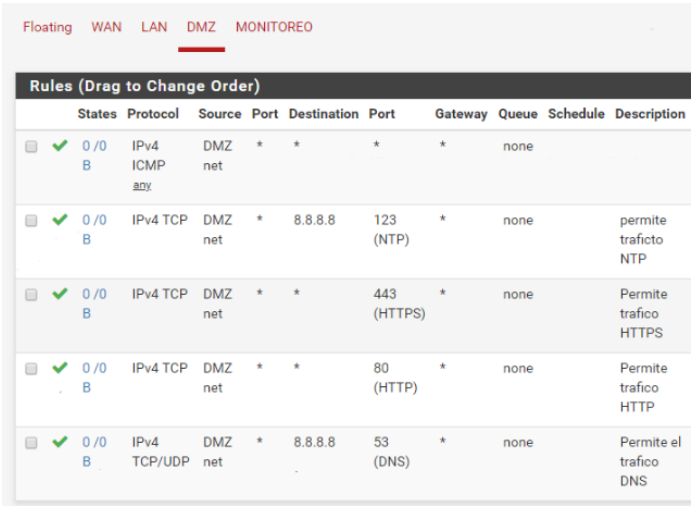
Floating WAN LAN DMZ MONITOREO

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓	4 /219 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
✓	0 /5.10 MiB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		
✓	0 /1.94 MiB	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		
✓	0 /9 KiB	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none		Default allow LAN to any rule
✓	0 /0 B	IPv4 ICMP any	LAN net	*	*	*	*	none		

Fuente: La investigación
Elaborado por: Autor

Ilustración 26: Reglas para interfaz DMZ, pfsense



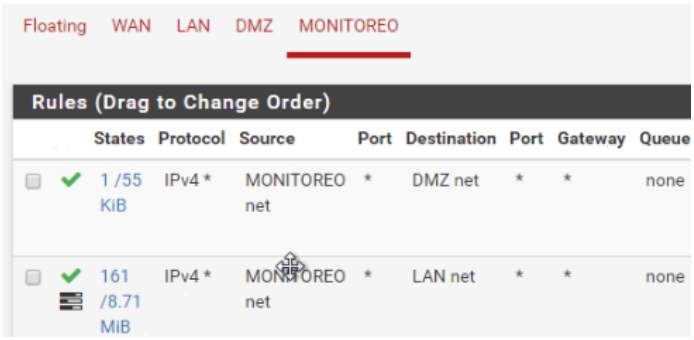
Floating WAN LAN DMZ MONITOREO

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓	0 /0 B	IPv4 ICMP any	DMZ net	*	*	*	*	none		
✓	0 /0 B	IPv4 TCP	DMZ net	*	8.8.8.8	123 (NTP)	*	none		permite traficto NTP
✓	0 /0 B	IPv4 TCP	DMZ net	*	*	443 (HTTPS)	*	none		Permite trafico HTTPS
✓	0 /0 B	IPv4 TCP	DMZ net	*	*	80 (HTTP)	*	none		Permite trafico HTTP
✓	0 /0 B	IPv4 TCP/UDP	DMZ net	*	8.8.8.8	53 (DNS)	*	none		Permite el trafico DNS

Fuente: La investigación
Elaborado por: Autor

Ilustración 27: Reglas para interfaz MONITOREO, pfsense



Fuente: La investigación
Elaborado por: Autor

Levantamiento de servidor Web Apache en la componente DMZ

El procedimiento realizado de configuración de los archivos necesarios para el levantamiento de una página web http sencilla. 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 28: Página web alojada en DMZ

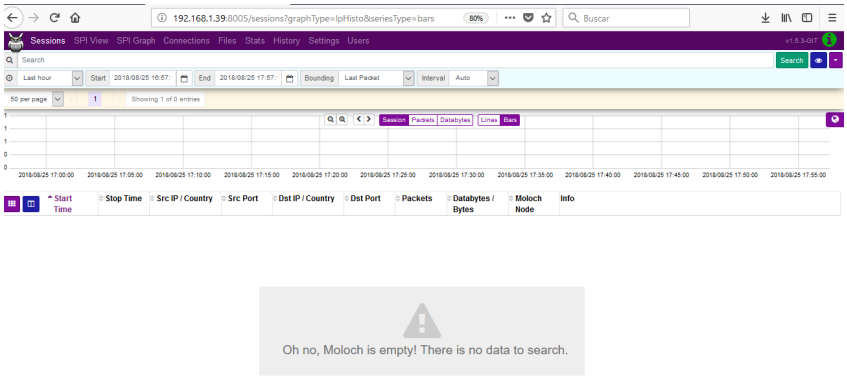
Fuente: La investigación
Elaborado por: Autor

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 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: ***'http:192.168.1.39/zabbix'***.

Ilustración 29: Web GUI de Moloch



Fuente: La Investigación
Elaborado por: Autor

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 de 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.

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.

Base de datos de malware para investigación

Fuente	Descripción	Última Actualización
Contagiodump[29]	Blog de recopilación de malwares categorizado bajo diferentes consideraciones (Tipo de malware, vulnerabilidad afectada, origen)	20/03/2018
Dasmalwerk[30]	Recopila malwares de diversas fuentes en internet.	16/04/2018

[29] http://contagiodump.blogspot.com/
[30] http://dasmalwerk.eu/

hybrid-analysis[31]	Herramienta gratuita de análisis híbrido automatizado de malware mediante Falcon Sandbox, permite subir muestras, analizarlas y compartirlas bajo suscripción, cual es gratuita para investigadores y académicos pero requiere de evaluación manual del perfil previo a la aceptación.	Actualizado
kernelmode[32]	Comunidad para discusión y peticiones de muestras de malwares con fines investigativos y académicos, requiere de invitación	Actualizado

[31] https://www.hybrid-analysis.com/
[32] http://www.kernelmode.info/forum/viewforum.php?f=16

malshare[33]	Repositorio de colección de malware para investigadores y resultados YARA (herramienta para clasificar e identificar muestras)	Actualizado
avcaesar[34]	Motor de búsqueda y análisis de muestras de malware a través de varios antivirus	Actualizado
thezoo.morirt[35]	Tiene el fin de acercar el análisis de malware al público en general, posee un repositorio en GitHub con diferentes tipos de muestras	08/02/2018
objective-see[36]	Base de datos para malware y adware con afectaciones a dispositivos Mac	No Actualizado

[33] https://malshare.com/
[34] https://avcaesar.malware.lu/
[35] http://thezoo.morirt.com/
[36] objective-see

virusign[37]	Repositorio de acceso restringido a muestras de malwares para el mejoramiento de softwares antivirus e investigación	Actualizado
beta.virusbay[38]	Tiene como objetivo la ayuda eficiente a organizaciones ante incidentes de seguridad. Necesita de invitación para el acceso a la base de datos.	Actualizado
virustotal[39]	Servicio gratuito de análisis de archivos y URLs sospechosos.	Actualizado

Fuente: La Investigación
Elaborado por: Autor

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*" [4].Para este proyecto se toma a consideración tanto «el enfoque masivo» análogo al marketing masivo o de la escopeta, y el

[37] http://www.virusign.com/
[38] https://beta.virusbay.io/
[39] https://www.virustotal.com/en/

«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 masivo; mientras, el componente DMZ, representando servicios empresariales, puede ser claro objetivo de malware dirigido.

Enfoque y características de muestras

Componente	*Enfoque*	*Características*
Intranet	Masivo	• Primera 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[40] o APT[41]. • Uso de encriptación en el transporte. • Posibilidad de realizar robo de información u obtención de credenciales.

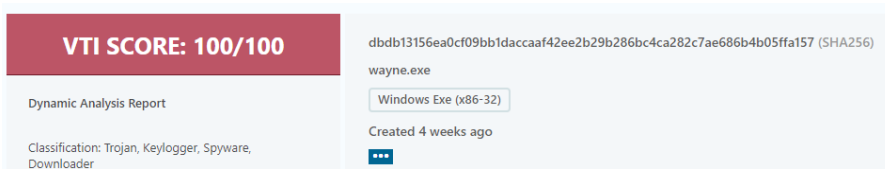
Fuente: La Investigación
Elaborado por: Autor

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 potente 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.

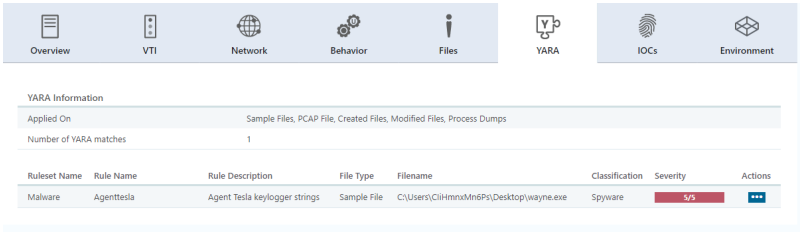
[40] Remote Access Tool
[41] Advanced persistent threat

Calificación obtenido por VMRAY



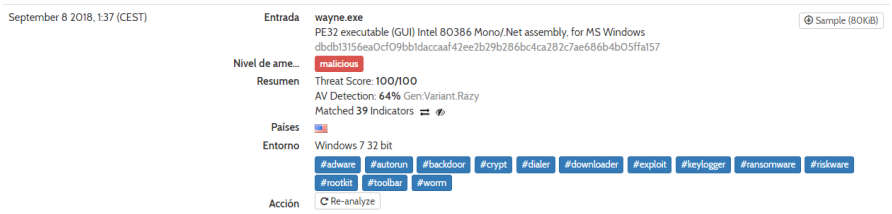
Fuente: vmray.com
Elaborado por: Autor

Ilustración 30: Origen de muestra "wayne.exe"



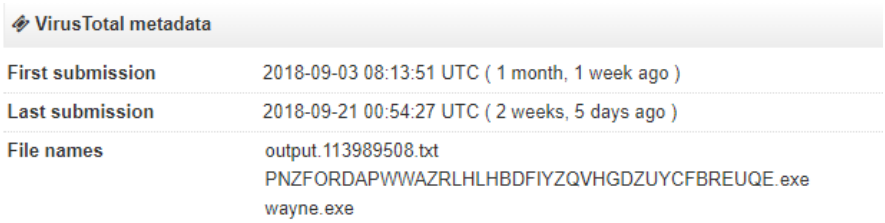
Fuente: vmray.com
Elaborado por: Autor

Espécimen propuesto para análisis en componente Intranet



Fuente: Hybrid-Analysis
Elaborado por: Autor

Primera aparición de muestra por VirusTotal



Fuente: VirusTotal.com
Elaborado por: Autor

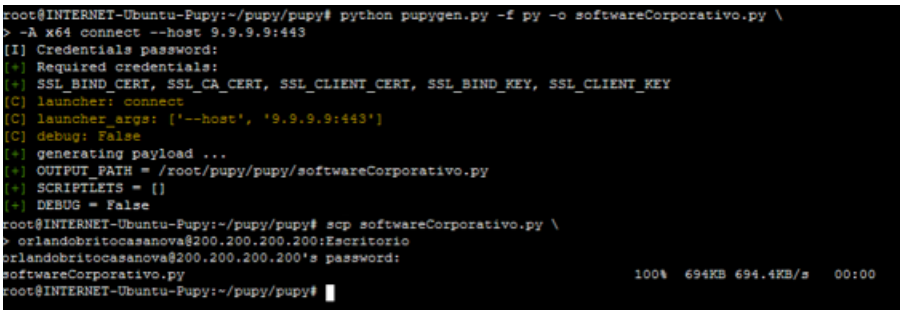
Espécimen para componente DMZ

Un malware objetivo se desarrolla enfocado en características específicas de la red o sistema a comprometer. Sus creadores más 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 **¡Error! No se encuentra el origen de la referencia.** se muestra 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.

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



Fuente: La investigación
Elaborado por: Autor

Introducción

El análisis dinámico de malware es crucial para conocer las capacidades, comportamiento y objetivos de software sospechosos, en donde el 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.

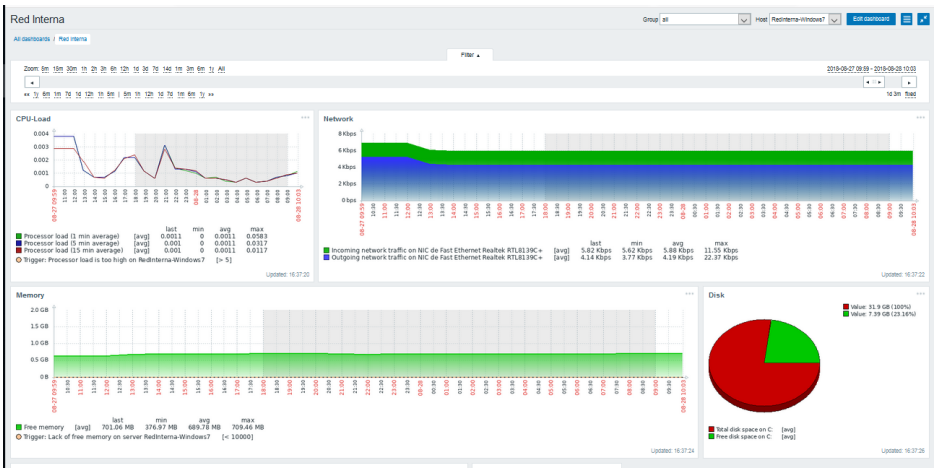
Análisis de estado previo del sistema en conjunto.

Al 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.

Análisis previo de red con implementación de INetSIM.

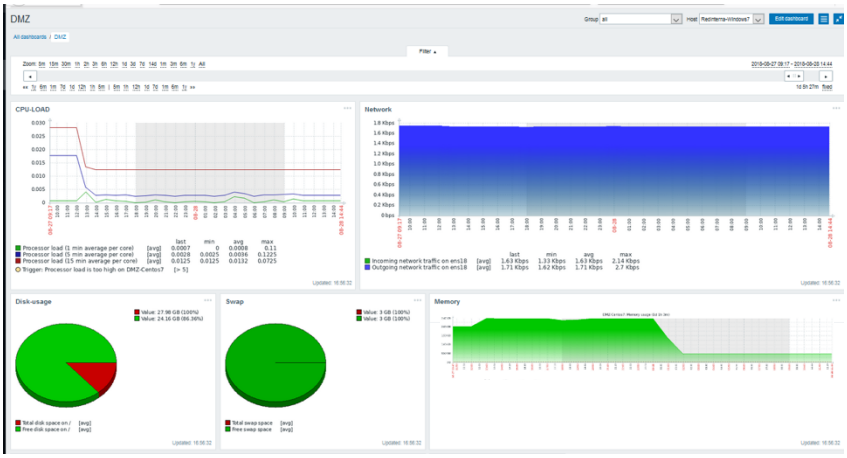
La medición se realizó en un periodo de veinticuatro horas, entre las 10:00 AM del 27/08/18 y 10:00 AM del 28/08/17.

Rendimiento de componente Intranet



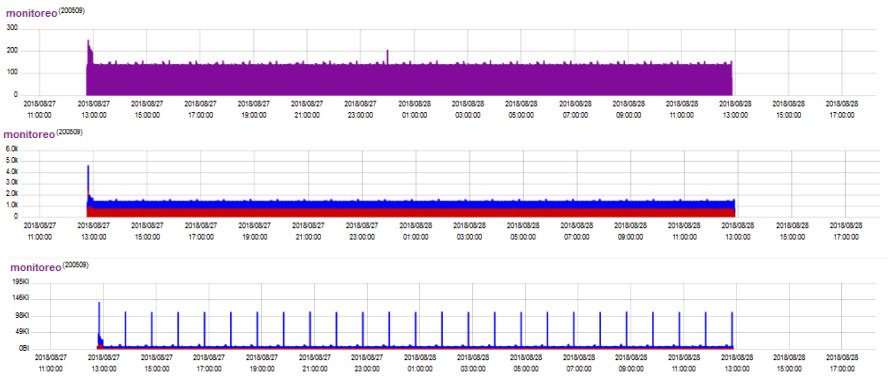
Fuente: La Investigación
Elaborado por: Autor

Rendimiento del componente DMZ



Fuente: La Investigación
Elaborado por: Autor

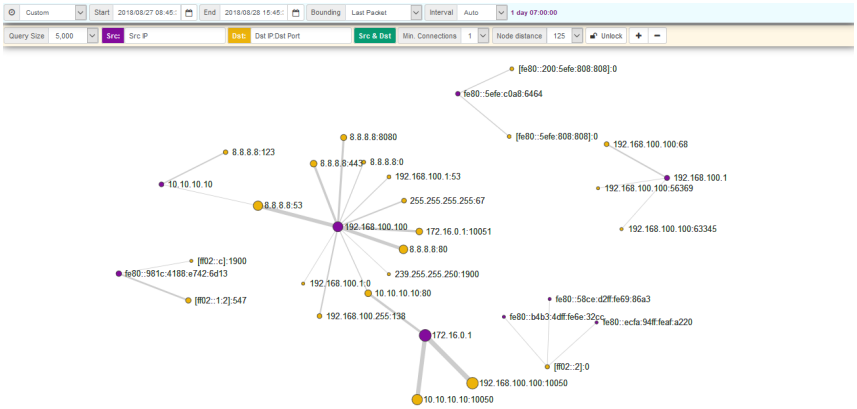
El estudio de los paquetes cursados por las redes objetivos (vmbr100 → Intranet y vmbr200 → DMZ) se realiza empleando la herramienta de escucha de paquete Moloch con base de datos Elasticsearch, en conjunto con el demonio "daemonlogger" ejecutado en el host hipervisor proxmox para realizar un mirror de paquetes cursados en las redes antes mencionadas a la red vmbr600.



Fuente: La Investigación
Elaborado por: Autor

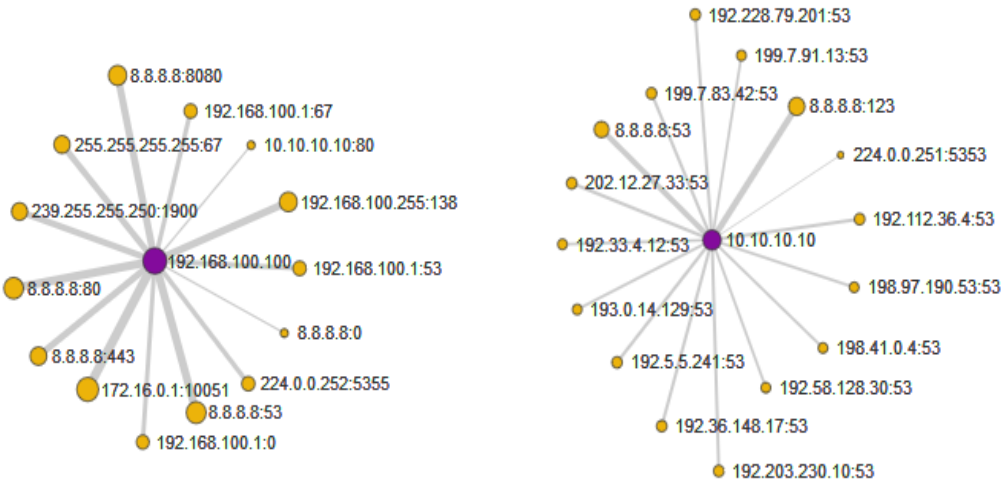
Las conexiones específicas e independientes de los componentes Intranet (192.168.100.100) y DMZ (10.10.10.10) respectivamente.

Diagrama de conexiones previo a infección



Fuente: La Investigación
Elaborado por: Autor

Diagrama de conexiones de componente Intranet y DMZ

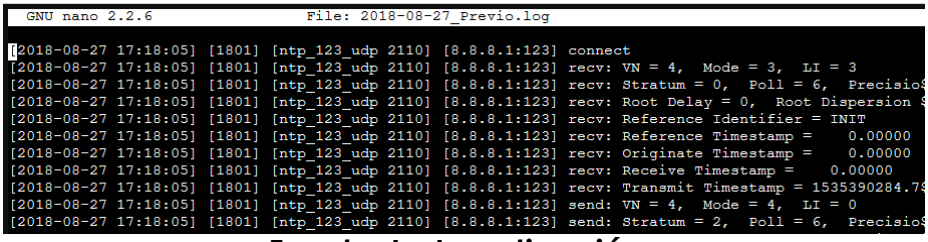


Fuente: La Investigación
Elaborado por: Autor

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'***.

Peticiones obtenidas por servidor INetSIM durante análisis previo infección

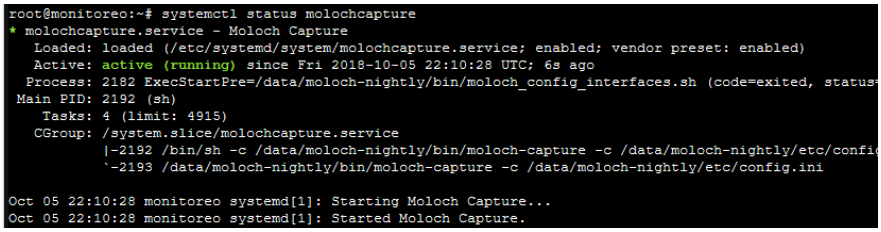


Fuente: La Investigación
Elaborado por: Autor

Análisis previo de red con salida a Internet.

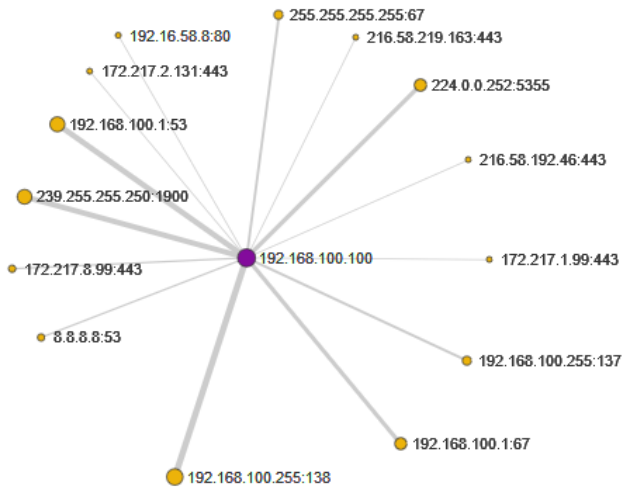
El análisis se enfocó al comportamiento del componente Intranet, al estar expuesto a malware desconocido y foráneo, contrario al componente DMZ, cual conexiones se encuentran establecidas.

Inicio de servicio molochcapture en componente Monitoreo



Fuente: La Investigación
Elaborado por: Autor

Conexiones establecidas durante análisis previo con salida a Internet



Fuente: La Investigación
Elaborado por: Autor

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).

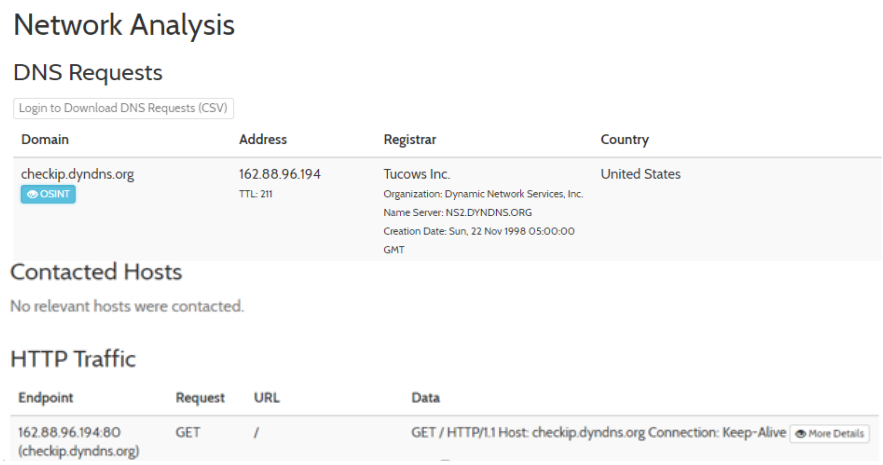
Análisis automático de muestra masivo "wayne.exe" mediante Hybrid-Analysis.

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": 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"»*

Análisis de red obtenido en Hybrid-Analysis



Fuente: Hybrid-Analysis.com
Elaborado por: Autor

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.

Extracto de escaneo por VirusTotal

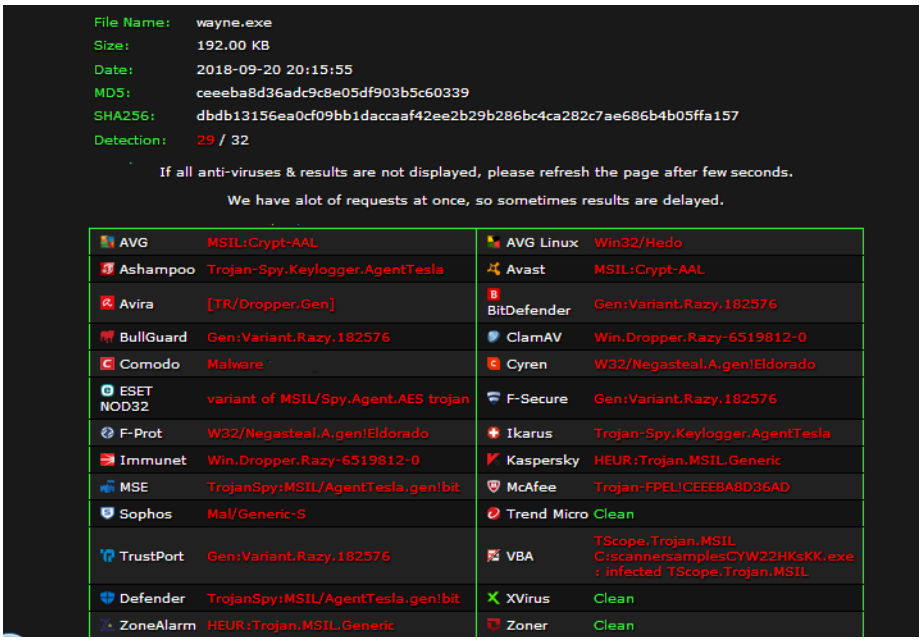
Antivirus	Resultado
Avast	MSIL:Crypt-AAL [Trj]
AVG	MSIL:Crypt-AAL [Trj]
BitDefender	Gen:Variant.Razy.182576
ClamAV	Win.Dropper.Razy-6519812-0
ESET-NOD32	a variant of MSIL/Spy.Agent.AES
Kaspersky	HEUR:Trojan.MSIL.Generic
Malwarebytes	Trojan.PasswordStealer.MSIL
McAfee	Trojan-FPEL!CEEEBA8D36AD
Panda	Trj/GdSda.A
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

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-escanner 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.

Escaneo de espécimen "wayne.exe" empleando Spyral Scanner



File Name: wayne.exe
Size: 192.00 KB
Date: 2018-09-20 20:15:55
MD5: ceeeba8d36adc9c8e05df903b5c60339
SHA256: dbdb13156ea0cf09bb1daccaaf42ee2b29b286bc4ca282c7ae686b4b05ffa157
Detection: 29 / 32

If all anti-viruses & results are not displayed, please refresh the page after few seconds.
We have alot of requests at once, so sometimes results are delayed.

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:scannersamplesCYW22HKsKK.exe : infected TScope.Trojan.MSIL
Defender	TrojanSpy:MSIL/AgentTesla.gen!bit	XVirus	Clean
ZoneAlarm	HEUR:Trojan.MSIL.Generic	Zoner	Clean

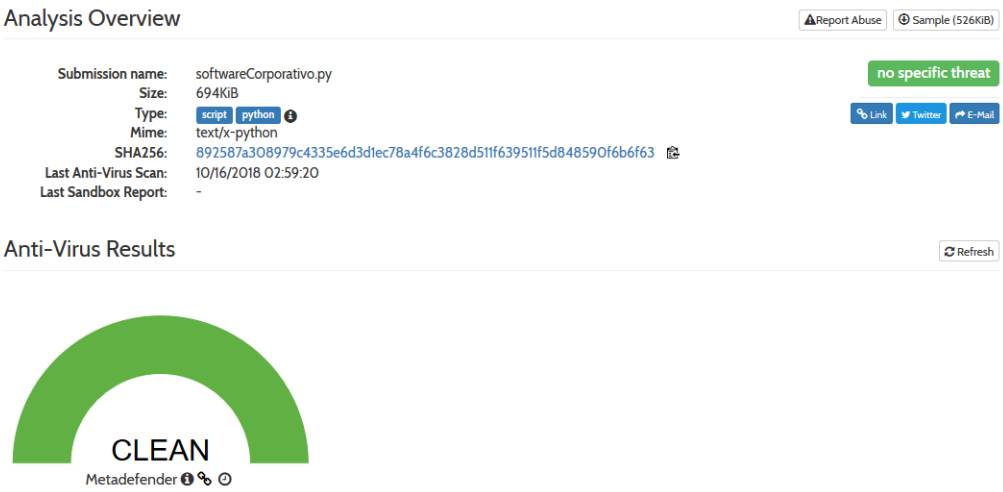
Fuente: Spyral Scanner
Elaborado por: Autor

Análisis automático de malware dirigido "softwareCorporativo.py" mediante Hybrid-Analysis.

Al ser un espécimen creado para desenvolverse en ambientes Linux primordialmente, es estableció el mismo como entorno de análisis automático usando las tecnología híbridas de Hybrid-Analysis, presenta la clasificación de no amenaza según el análisis realizado[42]. No obstante, existe errores en el transcurso de la ejecución de Falcon Sandbox, impidiendo la obtención de un reporte.

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

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

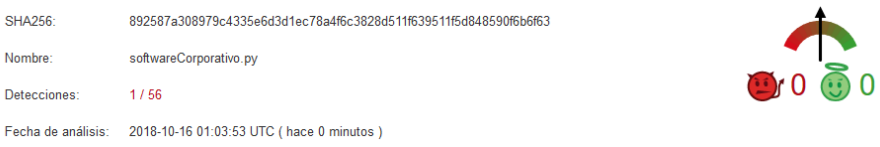


Fuente: Hybrid-Analysis
Elaborado por: Autor

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

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

Escaneo de muestra "softwareCorporativo.py" mediante VirusTotal

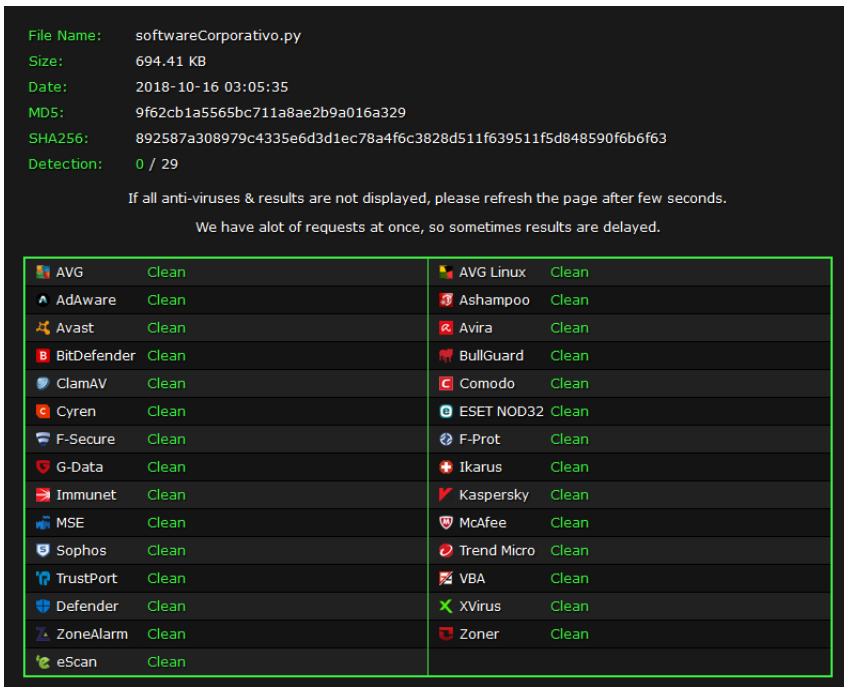


Fuente: VirusTotal.com
Elaborado por: Autor

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.

Escaneo de muestra "softwareCorporativo.py" mediante Spyral Scanner



Fuente: Spyral Scanner
Elaborado por: Autor

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.

Análisis dinámico empleando INetSIM.

La muestra de estudio se ejecutó a las 13:28 (GMT-5) y 20:40 hasta las 21:48 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.

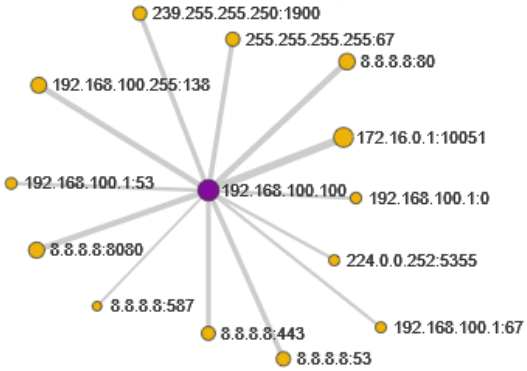
Evidencia el rendimiento del componente Intranet durante le ejecución del software.

Rendimiento de componente Intranet durante ejecución de "wayne.exe"

Fuente: La Investigación
Elaborado por: Autor

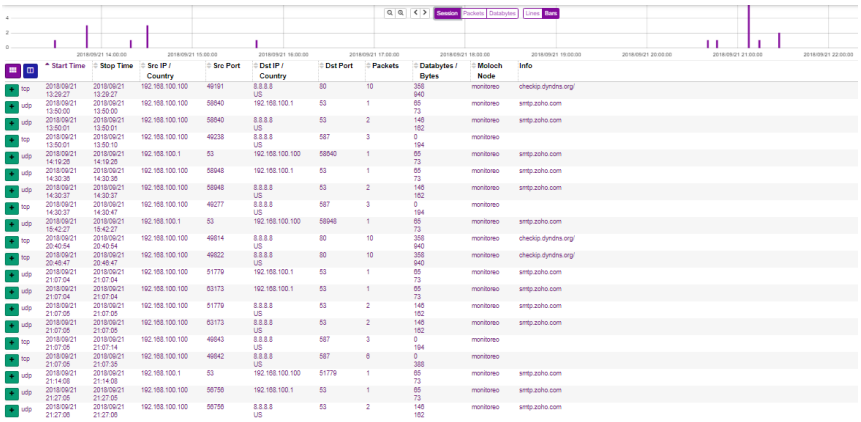
Exhibe las conexiones realizadas por la componente Intranet durante el periodo de evaluación. El carecimiento de direcciones ip diferentes corresponde al funcionamiento de INetSim, cual resuelve cada petición DNS con su propia ip, sin embargo existen conexiones inusuales al puerto 587 correspondiente al puerto «submission» del protocolo SMTP, pudiendo ser empleado en el envío de correo spam. ***¡Error! No se encuentra el origen de la referencia.*** muestra los paquetes capturados por Moloch e ***¡Error! No se encuentra el origen de la referencia.*** indica el contenido (vacío) de paquete con dirección puerto destino 587.

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



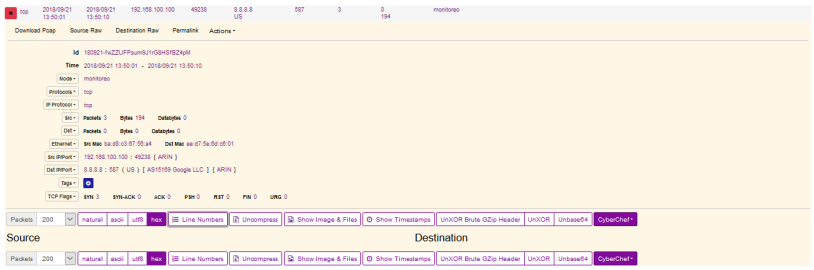
Fuente: La Investigación
Elaborado por: Autor

Paquetes obtenidos durante análisis de "wayne.exe" mediante Moloch



Fuente: La Investigación
Elaborado por: Autor

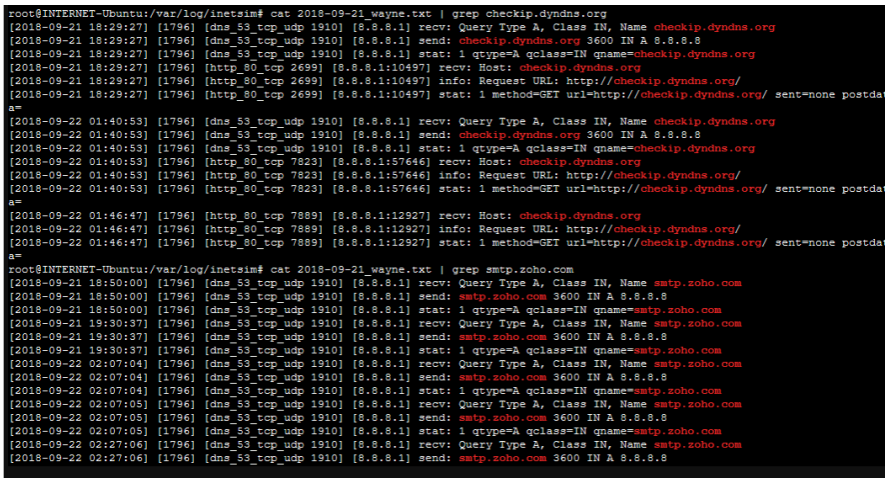
Paquete sospechoso con puerto destino 587



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 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'.

Peticiones y respuesta de INetSim a requerimientos de "wayne.exe"



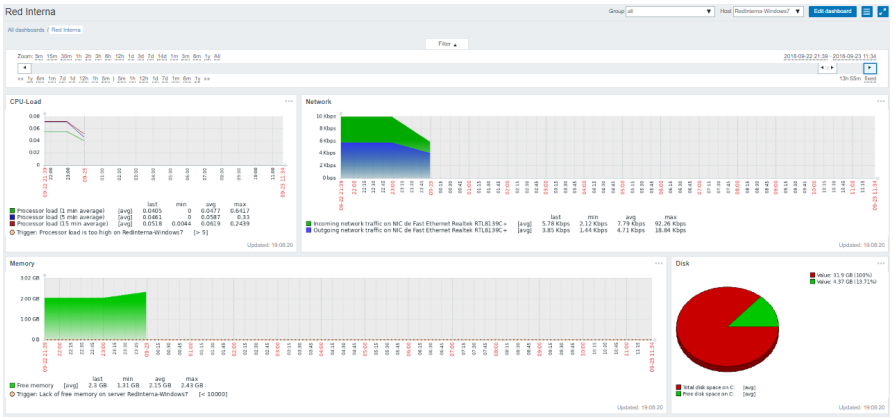
Fuente: La Investigación
Elaborado por: Autor

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 se justifica la realización de análisis dinámico con salida real a internet. Se realiza la

ejecución de la muestra en el transcurso de tiempo (desde 22/09/18 23:50:00, hasta 23/09/18 16:42:00).

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



Fuente: La Investigación
Elaborado por: Autor

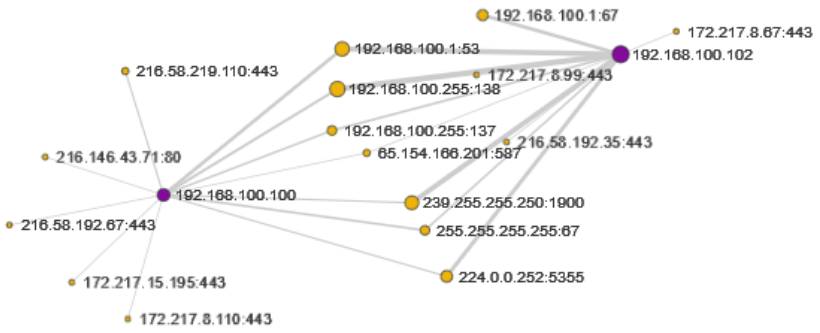
Cambio de dirección IP en componente Intranet

+	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:e742:6d13	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

Las conexiones realizadas por el componente Intranet con salida real a Intranet, obteniendo nuevas direcciones a estudiar y denotando el cambio de IP.

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

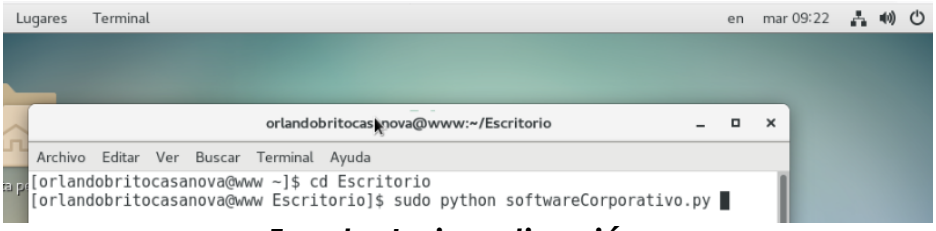


Fuente: La Investigación
Elaborado por: Autor

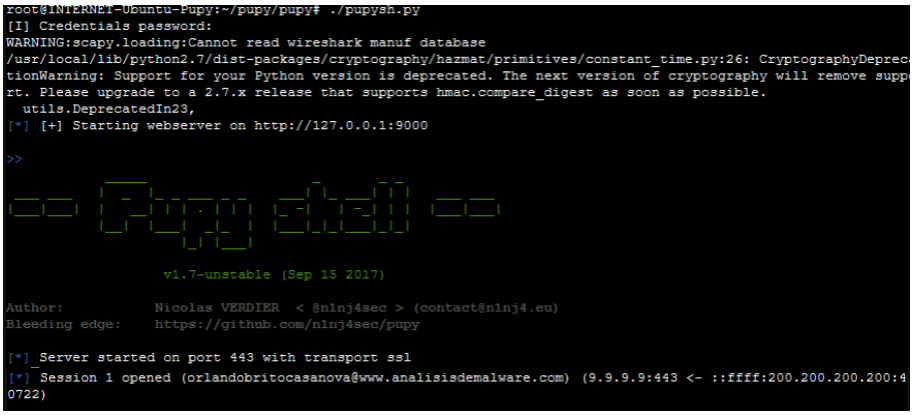
Análisis dinámico de muestra "softwareCorporativo.py" ejecutada en componente DMZ.

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. 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.

Ejecución de "softwareCorporativo.py" en componente INTRANET



Fuente: La investigación
Elaborado por: Autor



Fuente: La investigación
Elaborado por: Autor

Comportamiento de red y rendimiento de componente DMZ, durante ejecución de "softwareCorporativo.py"

El rendimiento interno del componente DMZ obtenido mediante el servicio Zabbix, 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.

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 [31], 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.

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).

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.

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.

Bibliografía

[1] kaspersky, «support.kaspersky.com,» 2018. [En línea]. Available: https://support.kaspersky.com/mx/789#block2. [Último acceso: 5 23 2018].

[2] Cisco, «Introducción a la ciberseguridad,» Cisco, 2018.

[3] ESET Latinoaméria , «ESET Security Report Latinoamerica 2017,» 2017.

[4] A. H. Michael Sikorski, «Practical Malware Analysis. The Hans-On Guide to Dissectin Malicious Software,» no starch press, San Francisco, 2012.

[5] Y. P. I. R. Syarif Yusirwan S, «Implementation of Malware Analysis using Static and,» *International Journal of Computer Applications (0975 – 8887),* vol. 117, nº 6, 2015.

[6] 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].

[7] A. Sanabria, «Malware Analysis: Environment Design and Artitecture,» SANS Institute, 2007.

[8] 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].

[9] 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].

[10] latam.kaspersky.com, «latam.kaspersky.com,» 2018. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/metamorphic-virus. [Último acceso: 24 5 2018].

[11] 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.

[12] I. L. R. C. HENRY CRISTHIAN MANCHENO TORRES, VULNERABILIDADES Y SEGURIDAD EN REDES TCP/IP, Guayaquil-Ecuador: Universidad Católica de Santiago de Guayaquil, 2013.

[13] D. F. A. VILLARUEL, Análisis Digital de una Infección de Malware en Sistemas Windows, Quito: Escuela Politécnica Nacional, 2016.

[14] S. O. Fernández, Análisis dinámico de malware ne entornos controlados, Madrid: Universidad Carlos III de Madrid, 2013.

[15] 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.

[16] T. M. J. Tene, Metodología para el análisis de malware en un ambiente controlado, Cuenca: Universidad Politécnica Salesiana Sede Cuenca , 2017.

[17] Cisco Networking Academy, Network Basics Companion Guide, Indianapolis: Ciscon Press, 2014.

[18] Cisco Systems, CCNA: INTODUCCIÓN A LAS REDES V.6.0, Indianapolis: Cisco Press, 2017.

[19] Univsersidad de Valencia , Sistema Industriales distribuidos, Valencia - España: Universidad de Valencia.

[20] A. S. Iyer, «Introduction to Enterprise Networks:,» de *IIT Bombay - Convergencia* , Bombay, 2005.

[21] wikipedia.org, «wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Virtualizaci%C3%B3n. [Último acceso: 12 6 2018].

[22] 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.

[23] 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].

[24] C. Z. S., «LA VIRTUALIZACIÓN, TIPOS DE VIRTUALIZACIONES,» Universidad Ecotec, 2012.

[25] 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].

[26] wikipedia, «wikipedi,» [En línea]. Available: https://es.wikipedia.org/wiki/Windows_Virtual_PC. [Último acceso: 5 6 2018].

[27] 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.

[28] C. E. M. Álvarez, Metodología: Diseño y desarrollo del proceso de investigación con énfasis en ciencias empresariales, México D.F: Limusa, 2011.

[29] 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].

[30] 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].

[31] I. Sridhar, «Introduction to Enterprise Networks:,» de *IIT Bombay - Convergencia*, Bombay, 2005.

[32] 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].

[33] 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/.

[34] V. Mohan, A Guide to Enterprise Network Monitoring, SolarWinds Worldwide, LLC., 2015.

[35] A. Cecil, «A Summary of Network Traffic Monitoring and Analysis,» cse.wustl.edu, 2006.

[36] 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].

[37] S. C. Rakesh Kumar, «An Importance of Using Virtualization Technology in Cloud Computing,» de *Global Journal of Computers & Technology* , Jaipur - India, 2015.

[38] pve.proxmox.com, «pve.proxmox.com,» 17 07 2017. [En línea]. Available: https://pve.proxmox.com/wiki/System_Requirements. [Último acceso: 30 07 2018].

[39] windowsreinstall.com, «windowsreinstall.com,» [En línea]. Available: http://windows7.windowsreinstall.com/systemrequirements.htm. [Último acceso: 30 07 2018].

[40] help.ubuntu.com, «ubuntu.com,» 13 10 2017. [En línea]. Available: https://help.ubuntu.com/community/Installation/SystemRequirements. [Último acceso: 30 07 2018].

[41] 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].

[42] pfsense, «pfsense.org,» [En línea]. Available: https://www.pfsense.org/products/. [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].

Descubre tu próxima lectura

Si quieres formar parte de nuestra comunidad,
regístrate en **https://www.grupocompas.org/suscribirse**
y recibirás recomendaciones y capacitación

compÁs

Grupo de capacitación e investigación pedagógica

@grupocompas.ec
compasacademico@icloud.com

compAs
Grupo de capacitación e investigación pedagógica

@grupocompas.ec
compasacademico@icloud.com

ISBN: 978-9942-33-200-4

@grupocompas.ec
compasacademico@icloud.com

compAS
Grupo de capacitación e investigación pedagógica