Fecha de presentación: septiembre, 2020, **Fecha de Aceptación**: noviembre, 2020, **Fecha de publicación**: enero, 2021

14

ANÁLISIS DINÁMICO DE MALWARE EN AMBIENTE DE RED VIRTUALIZADO

DYNAMIC ANALYSIS OF MALWARE IN A VIRTUALIZED NETWORK ENVIRONMENT

Emilio Zhuma Mera[1]
E-mail: ezhuma@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-3086-1413
Orlando Jesús Brito Casanova[1]
E-mail: orlando.brito2013@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-2051-5031
José Tubay Vergara[1]
E-mail: jtubay@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-2377-0716
Byron Oviedo Bayas[1]
E-mail: boviedo@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-5366-5917
[1] Universidad Técnica Estatal de Quevedo. Ecuador.

Cita sugerida (APA, séptima edición)

Zhuma Mera, E., Brito Casanova, O. J., Tubay Vergara, J., & Oviedo Bayas, B. (2021). Análisis dinámico de malware en ambiente de red virtualizado. ***Revista Conrado, 17(78)***, 113-120.

RESUMEN

La presente investigación estudia la creación de un entorno de red virtual para la realización de análisis dinámico de malware empleando el sistema hipervisor Proxmox y tecnologías de virtualización LXC o KVM/QEMU para el aseguramiento de la operatividad y el correcto aislamiento de los componentes. Se propone una topología modesta de seguridad perimetral empleando una DMZ con cortafuego en trípode, red interna y añadiendo una red de monitoreo, como representación de ambiente empresarial a nivel pequeño o mediano 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. Según las características de zonas con gran importancia operacional (red interna y DMZ), son asechadas por código maliciosos clasificados de acuerdo al alcance esperado: masivos y dirigidos. El uso de herramientas externas para el desarrollo y obtención de datos necesarios sobre el comportamiento del sistema infectado y el desenvolvimiento del espécimen en ejecución con servicios como Zabbix y Moloch poseen limitaciones influyentes en la precisión del análisis dinámico y la consecuencia formulación de conclusiones y elaboración de indicadores de compromisos o firmas que ayuden a la detección de software maligno.

Palabras clave:

LXC, Malware masivo, Malware dirigido, Proxmox, QEMU.

ABSTRACT

The present research studies the creation of a virtual network environment to perform dynamic malware analysis using the Proxmox hypervisor system and LXC or KVM / QEMU virtualization technologies to ensure the operability and correct isolation of the components. A modest perimeter security topology is proposed using a DMZ with a tripod firewall, internal network and adding a monitoring network, as a representation of the business environment at a small or medium level for the abstraction in minimum elements permissible to virtualize with the least impact on the system functionality and safeguarding the consumption of physical resources. According to the characteristics of areas with great operational importance (internal network and DMZ), they are haunted by malicious code classified according to the expected scope: massive and targeted. The use of external tools to develop and obtain the necessary data on the behavior of the infected system and the development of the specimen in execution with services such as Zabbix and Moloch have influential limitations on the precision of the dynamic analysis and the consequent formulation of conclusions and elaboration of “Indicators of compromise” or signatures that aid in the detection of malicious software.

Keywords:

LXC, Mass Malware, Targeted Malware, Proxmox, QEMU.

INTRODUCCIÓN

Las organizaciones gubernamentales o empresariales poseen muchos retos respecto a temas de seguridad, son el blanco predilecto de ciber-delincuentes en búsqueda de cuantiosas ganancias económicas o un impacto negativo de la confiabilidad y participación en el mercado de grandes corporaciones por diversas motivaciones. Una de las principales amenazas surge con las infecciones de malware en redes corporativas, donde, estos son códigos maliciosos diseñados para vulnerar sistemas y causar perjuicios significativos, sea con fines monetarios, activismo e incluso terrorismo. El análisis dinámico debe realizarse en un laboratorio con ambiente controlado, debido a las dificultades económicas y logísticas de un laboratorio físico, la opción más usada es la simulación del entorno, usando para ello softwares de virtualización, permitiendo facilidades como: Obtención de capturas de estado del sistema (snapshots), restablecimiento del sistema, menor riesgos a equipos reales, minoración en costos de investigación. La virtualización es una tecnología de gran importancia presente y futura, debido a todas sus prestaciones para con la interoperabilidad de servicios y su aplicación como base de tecnologías en la nube. El reporte anual titulado ESET Security Report Latinoamérica 2018 (Enjoy Safer Tecnology, 2018) manifiesta como una de cada cinco empresas Latinoamericanas estuvieron propensas a por lo menos un incidente de seguridad, aumentando respecto a años anteriores, siendo el software maligno líder con un 45%. Ecuador reporta un 22% de infecciones producidas por ransomware convirtiéndose en cabeza de la lista.

El malware puede estar dirigidos a objetivos generales o destinados a quebrantar una determinada empresa u organismo de diverso tipo, motivo de gran inquietud dentro del mundo empresarial, por ello, Enjoy Safer Tecnology (2017), en su encuesta titulada Security Report Latinoamérica 2017 , denota como principal preocupación la infección por software malicioso con un 56%, esto debido al ***"grado de sofisticación que tiene el malware y el retorno económico que genera".*** La sofisticación de nuevos softwares maliciosos disminuye la efectividad de sistemas de seguridad, como antivirus, basados en el conocimiento del comportamiento y efectos del malware, necesitando de investigación y monitoreo de sistemas para su detección. Las empresas pequeñas, medianas e inclusive grandes, generalmente carecen de capital para poseer equipos de respuestas propios, siendo propensas a software maligno no detectado por soluciones de seguridad como antivirus, al trabajar usualmente con firmas digitales cimentadas en el comportamiento.

Zeltser (2014), considera 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".*** Los elevados costos de implementación de un laboratorio físico de análisis exceden las posibilidades para empresas con recursos limitados o investigadores independientes, por lo cual las aplicaciones de esta tecnología al mundo de análisis de malware son indispensables, planteando: ¿En qué medida las posibilidades brindadas por entornos virtuales permiten el análisis dinámico de malware y el estudio del impacto a la red corporativa como conjunto?

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

DESARROLLO

La investigación se estructuró de acuerdo a los objetivos, sistematizando en orden lógico que sirva de base para definir o establecer cualidades dependientes de las distintas etapas del trabajo, cuales son llamadas fases e involucran un enfoque declarado según los objetivos específicos. Estas fases son:

- Fase uno: Identificación de topología. – Al definir características comunes entre topologías de red lógicas de amplio uso entre empresas pequeñas, medianas o sucursales de grandes corporaciones, se estableció un punto de partida sólido para la realización de abstracción mínima de acuerdo a cada componente resultante para salvaguardar los recursos necesarios en la virtualización y operación de la red, manteniendo los requerimientos al mínimo permisible sin afectar la operatividad del entorno. 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 de amplio uso.
- Fase dos: Virtualización de topología. – Se estableció los requisitos de virtualización de los diferentes elementos abstraídos y virtualizables durante la fase previa,

la elección de tecnología de virtualización según características y objetivos del componente en el marco del análisis dinámico, instalación de los sistemas operativos necesarios y sus servicios, e interconexión y aislación de las redes establecidas empleando adaptadores de red "bridge", análogos a conmutadores virtuales. Se propuso las siguientes directrices para la elección de una plataforma de virtualización:

» 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.

- Fase tres: Identificación de muestras. – El estudio de las características y finalidades de los componentes de red establecidos sirvió en la definición pertinente de malware según las principales zonas críticas: componte de "red interna" (malware masivo); y, componente "zona desmilitarizada" (malware dirigido). La obtención de ejemplares de malware de amplio alcance fue facilitada mediante la base de datos del sistema automático de análisis distribuido Hubrid-Analysis, mientras que se empleó una herramienta de control remoto (RAT) como generador de código con intenciones maliciosas según características propias de su componente objetivo.
- Fase cuatro: Análisis dinámico de malware. – Se categorizó como análisis dinámico externo al emplearse como herramientas de obtención de información una componente denominada "monitoreo" con servicios como "Zabbix" (analizador remoto de sistemas), y "Moloch" (capturador de paquetes), tanto para el establecimiento de una línea base, así como la respectiva comparación de los resultados obtenidos con herramientas en línea (hybrid-analysis, VirusTotal, Spyral Scanner).

En las tablas 1 y 2 se especifica brevemente los recursos hardware y software empleados.

Tabla 1. Recursos Hardware empleado.

#	Equipo	Descripción
1	Computadora portátil. (empleada como servidor de virtualización)	Hp Pavilion 15r210dx • Intel® Core™ I5-5200U 2.20 GHz – 4 núcleos • 698.7 GB de disco duro • 8 GB de RAM
1	Router doméstico (Salida real a internet)	Cisco Linksys E1200

Tabla 2. Recursos Materiales y software empleado.

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

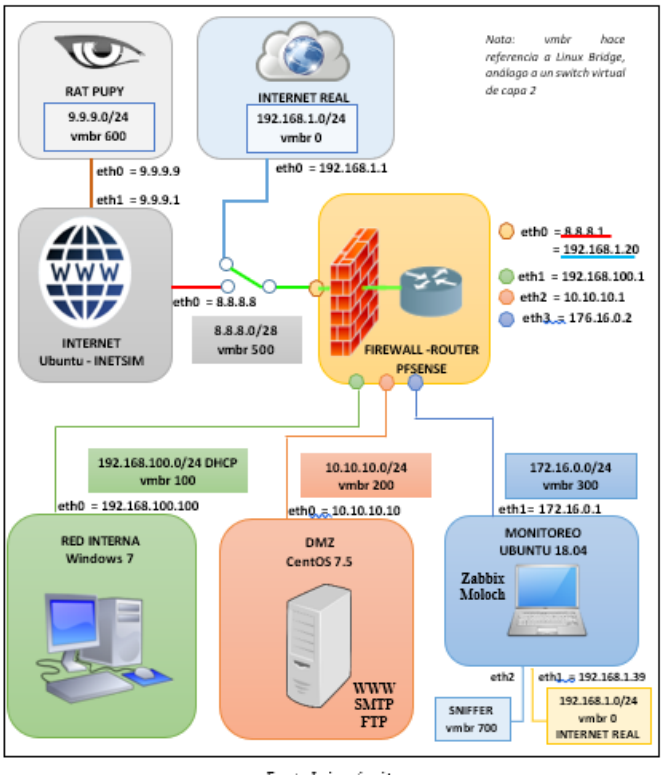


Figura 1. Topología lógica de red empresarial a implementar.

Dentro de los resultados obtenidos en fase uno se tiene: Identificación de topologías. – No es necesario la creación

de una topología de gran tamaño si las funcionalidades son abstraídas según cada componente, representándolos en una entidad única; debido a los fines de la actual investigación es necesario representar una arquitectura funcional, con capacidades de empleo en análisis dinámico de software malicioso.

Se opta por la utilización de una modesta topología de seguridad perimetral de amplio uso empleando una DMZ con un cortafuego en trípode como la expuesta por Cross (2018), siendo abstracción de una red empresarial, según la categorización por tamaño (Iyer, 2005), adicionando una red de monitoreo. De manera siguiente se expone el nombre del componente y sistema operativo optado.

- Red Interna: Microsoft Windows 7 Ultimate Service Pack 1 64 bits. La Figura 1 presenta el diagrama lógico de la topología a virtualizar.
- DMZ: CentOS Server 7.5 64 bits
- Firewall – Router: Pfsense Community Edition 2.4.3 64 bits.
- Internet: INetSim 1.2.8 released 2018-06-12 ejecutado en Ubuntu 14.04.2
- Monitoreo: Ubuntu 18.04.1 LTS 64 bits; Zabbix; Moloch.

En la fase dos se obtienen los siguientes resultados: Virtualización de topología. – ***"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"*** (Kumar & Charu, 2015). 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. La Tabla 3 fue usada como referencia para elección del hipervisor Proxmox en su versión 5.2, al contar con características que facilitan el monitoreo tanto del entorno completo como de cada elemento independiente, con posibles aplicaciones en análisis dinámico de malware.

Tabla 3. 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.
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 (Kumar & Charu, 2015).
Arquitectura	Hipervisor	Permite que varios S.O. se ejecuten simultáneamente en un solo host físico, así como, proporciona abstracción de hardware al SO huésped (Guest OS) y multiplexa de manera eficiente los recursos de hardware subyacentes (Kumar & Charu, 2015).

Proxmox virtualiza elementos usando dos tecnologías, cuales poseen cualidades diferentes haciéndolas indicadas para cierto tipo de máquina virtual según los requerimientos. Estas tecnologías son: LXC (usado en la implementación de containers CT), permite la ejecución de un sistema operativo completo dentro del núcleo del hipervisor, esto limita las capacidades, restringe su uso a sistemas operativos de núcleo Linux, pero, permite un mejor ahorro de recursos (CPU, RAM); QEMU/KVM (usado en implementación de VM), emula un computador físico con sus recursos, particiones, archivos, tarjetas de red, como si fuera un dispositivo real. En la Tabla 4, se presenta la elección de sistema de virtualización para los componentes de la red empresarial con su respectiva justificación.

Tabla 4. Elección de sistema de virtualización (CT - VM).

Tecnología	Elementos	Justificación
CT (LXC)	Ubuntu 14.04 para implementación de servicio INetSim, servidor Pupy y de Monitoreo	La creación de un container limita las capacidades, pero optimiza los recursos, esta tecnología puede ejecutar procesos de pocos requerimientos, por ello se decide su utilización para el levantamiento del servicio INetSim (emulación de Internet), RAT 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 Windows 7 y Pfsense (FreeBSD.

Dentro de los resultados obtenidos en fase tres se tienen: Identificación de muestras. – ***"Los malware pueden clasificarse según el enfoque del atacante respecto a la masificación de su código malicioso y el objetivo del mismo"*** (Sikorski & Honig, 2012). Este proyecto considera tanto el enfoque masivo análogo al marketing masivo o de la

escopeta, y el malware dirigido diseñado específicamente para atacar no más que la red de una organización, conociendo vulnerabilidades propias de la misma. El componente Intranet posee características de software masivo, tanto con uso doméstico como empresariales; mientras, el componente DMZ, representando servicios empresariales, puede ser claro objetivo de malware dirigido. La Tabla 5 presenta las características de las muestras elegidas.

Tabla 5. Descripción de muestras empleadas.

Nombre	Tipo	Objetivo	Fuente	Descripción
Wayne.exe	Masivo	Red Interna	Hybrid-analysis	Estudiada a profundidad en vmray.com, establecido en como generado por Agent Tesla , analizado por Hybrid-Analysis el 8 de septiembre de 2018; y, expuesto por primera vez por VirusTotal el 3 de septiembre de 2018.
Software-cor-porativo.py	Dirigido	DMZ	Generado mediante pupy	Posee características propias del sistema a vulnerar, Creado mediante el comando: 'python pupygen.py -f py -o softwarecorporativo.py -A x64 connect –host 9.9.9.9:443'

Como resultados de la fase cuatro se tienen: Para estudiar el desenvolvimiento de las muestras, se tomaron mediciones en plazos de veinte-cuatro horas, siendo analizadas las mismas en caso de presentar comportamiento que infiera la ejecución en un mayor tiempo o la salida a internet real para una mejor comprensión.

Explicación de monitoreo. – Parte imprescindible en cualquier tipo de análisis, al mantener redes separadas mediante bridge proporcionados por Proxmox, es necesario realizar las configuraciones pertinentes e idealizar una estrategia de acción conforme el comportamiento del malware así lo requiera. El servicio Zabbix necesita de un agente instalado en el sistema a monitorear, este es multiplataforma y de fácil configuración por lo cual simplemente debe de asegurarse que el componente firewall-router, posea las reglas de filtrado necesarias. El capturador de paquete Moloch, es un sniffer que puede escuchar los paquetes que transitan por unas de sus redes locales, al estar en redes ajenas a los componentes de estudio, se idealizó el uso del demonio "daemonlogger" instalado en el sistema Proxmox y controlado mediante línea de comando para espejar los paquetes que transitan por una red determinada hacia otra. Las redes vmbr100 (red interna) y vmbr200 (DMZ) son espejada hacia la red vmbr700 (monitoreo).

Análisis automático y escáner: "wayne.exe". – Fue analizado mediante Hybrid-Analysis, obteniendo valoración de malicioso e indicativos de: Adware, autorun, backdoor, crypt, dialer, downloader, exploit, keylogger, ransomware, riskware, rootkit, toolbar y worm. Mientras, mostró una ratio de detección de 46/67 por VirusTotal y 29/32 por Spyral-Scanner, comprobándose con estas herramientas la peligrosidad del código.

Análisis automático y escáner: "softwarecorporativo.py". – En su análisis por Hybrid-Analysis, se presenta la clasificación de "no amenaza" según el análisis realizado. No obstante, existe errores en el transcurso de la ejecución de Falcon Sandbox, impidiendo la obtención de un reporte. Informe completo en En tanto para los escáneres VirusTotal y Spyral-Scanner, denotan una ratio de detección muy bajo, 1/56 y 0/20 respectivamente.

Análisis dinámico de muestra "Wayne.exe" en componente Intranet. – Al ser un código desconocido a primera mano, fue necesario su ejecución según dos escenarios: mediante el uso de InetSim y, salida real a internet. Los datos recopilados por las herramientas de monitoreo son mostradas en la Figura 2, 3 y 4.

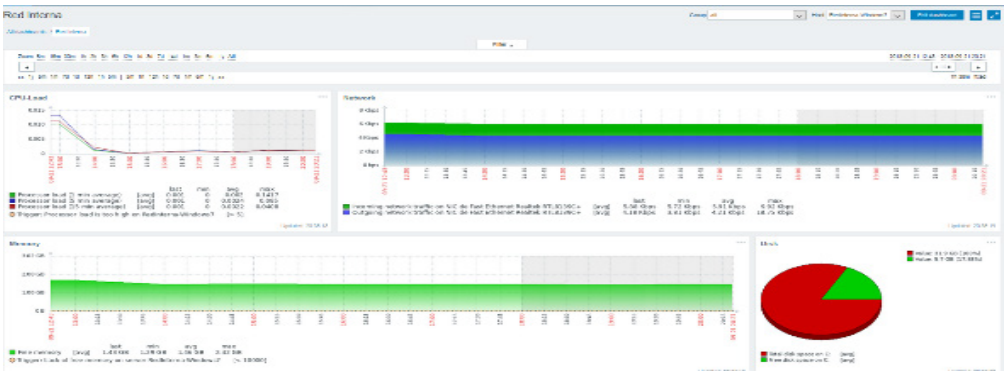


Figura 2. Rendimiento de componente Intranet durante ejecución de "wayne.exe".

Figura 3. Conexiones establecidas por componente Intranet durante ejecución de “wayne.exe”.

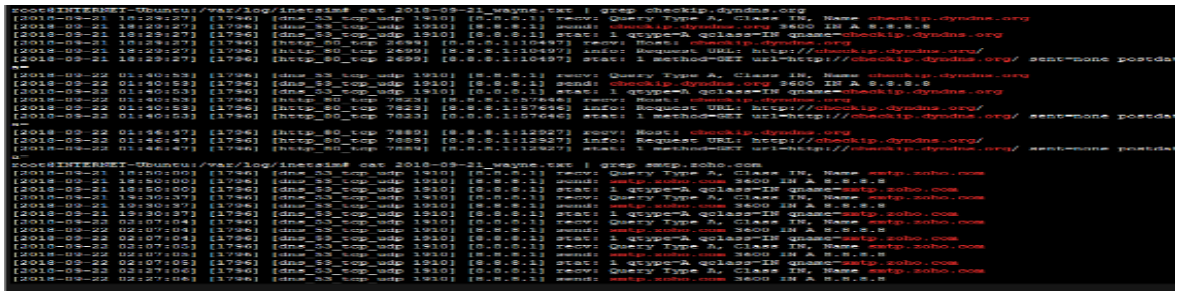


Figura 4. Peticiones y respuesta de INetSim a requerimientos de “wayne.exe”.

Análisis dinámico de muestra “softwarecorporativo.py” en componente DMZ. – Está fue realizada mediante la ejecución del servidor Pupy como herramienta de control remota, cual al ser monitoreada se demuestra la peligrosidad de estas plataformas de generación de malware en manos inescrupulosas (Figuras 5, 6 y 7).

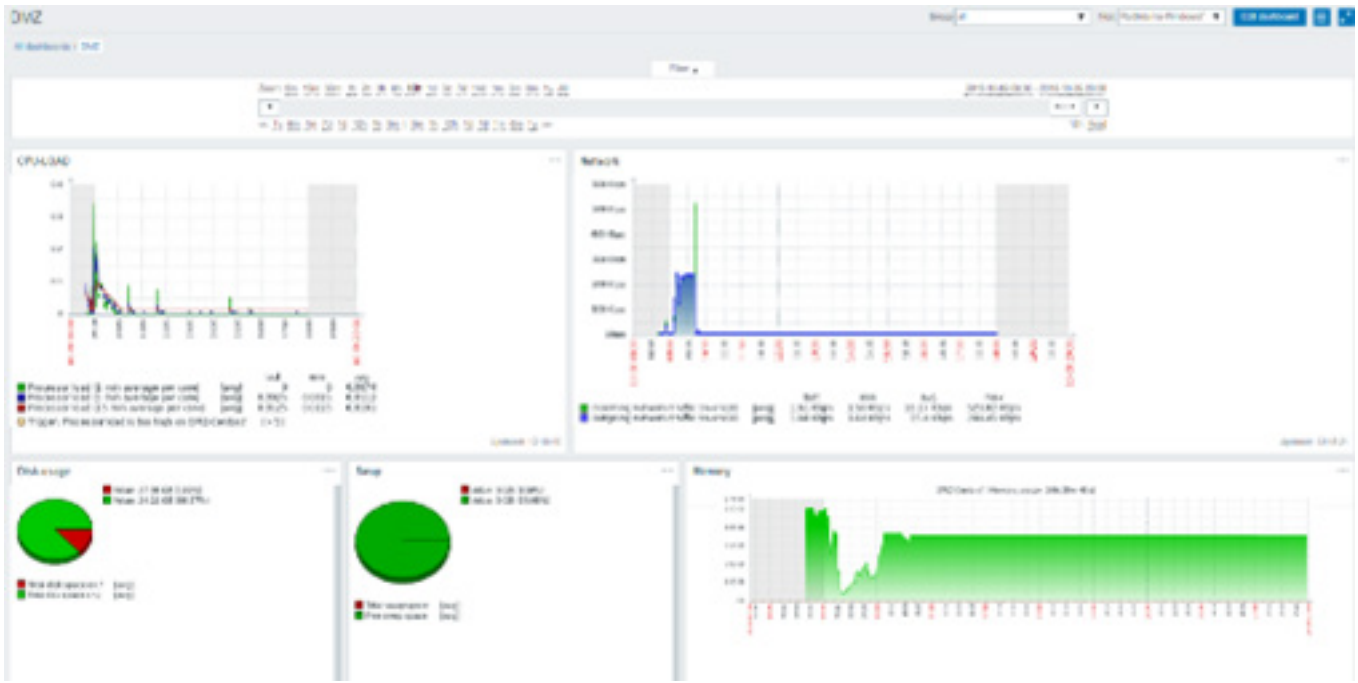
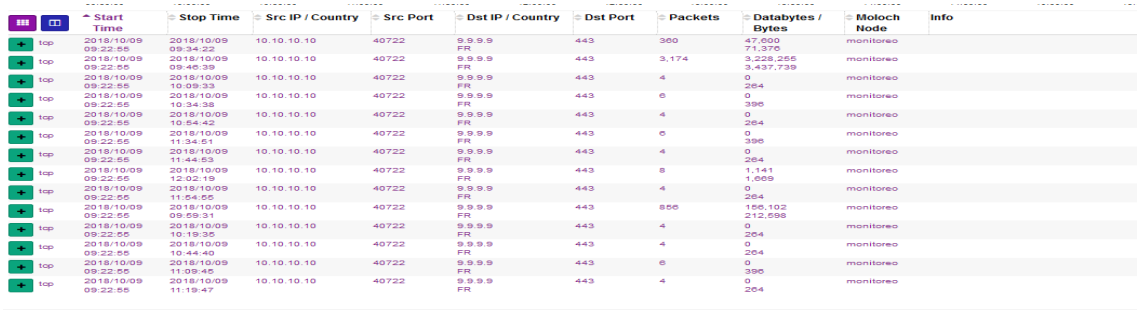


Figura 5. Rendimiento de componente DMZ durante ejecución de “softwareCorporativo.py” mediante Zabbix.



Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info
tcp 2018/10/09 09:22:55	2018/10/09 09:34:22	10.10.10.10	40722	9.9.9.9 FR	443	360	47,600 71,376	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 09:45:39	10.10.10.10	40722	9.9.9.9 FR	443	3,174	3,228,255 3,437,739	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 10:09:33	10.10.10.10	40722	9.9.9.9 FR	443	4	0 264	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 10:34:38	10.10.10.10	40722	9.9.9.9 FR	443	6	0 396	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 10:54:42	10.10.10.10	40722	9.9.9.9 FR	443	4	0 264	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 11:34:51	10.10.10.10	40722	9.9.9.9 FR	443	6	0 396	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 11:44:53	10.10.10.10	40722	9.9.9.9 FR	443	4	0 264	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 12:02:19	10.10.10.10	40722	9.9.9.9 FR	443	8	1,141 1,669	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 11:54:55	10.10.10.10	40722	9.9.9.9 FR	443	4	0 264	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 09:59:31	10.10.10.10	40722	9.9.9.9 FR	443	856	156,102 212,698	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 10:19:35	10.10.10.10	40722	9.9.9.9 FR	443	4	0 264	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 10:44:40	10.10.10.10	40722	9.9.9.9 FR	443	4	0 264	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 11:09:45	10.10.10.10	40722	9.9.9.9 FR	443	6	0 396	monitoreo	
tcp 2018/10/09 09:22:55	2018/10/09 11:19:47	10.10.10.10	40722	9.9.9.9 FR	443	4	0 264	monitoreo	

Figura 6. Paquetes obtenidos pom,mr Moloch durante ejecución de “softwareCorporativo.py”.

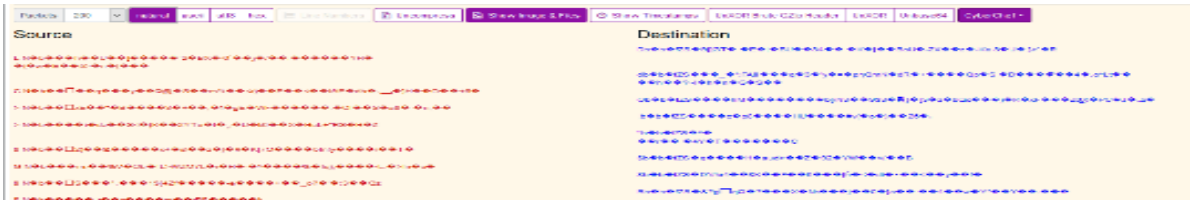


Figura 7. Muestra de contenido de paquete obtenido durante ejecución de “softwareCorporativo.py”.

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). La Figura 8 muestra ejecución de topología usando tecnología LXC y KVM, mientras, que la Figura 9 expresa el empleo de igual número de máquinas virtuales únicamente con KVM.

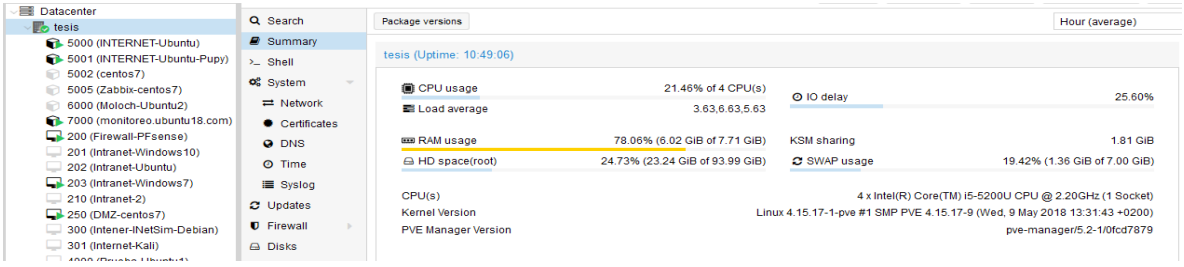


Figura 8. Ejecución de topología con técnicas LXC-KVM.

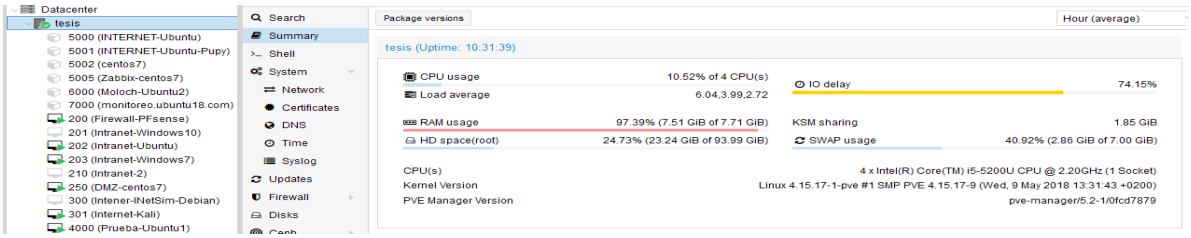


Figura 9. Ejecución de topología únicamente con tecnología KVM.

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 transferencias 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.

CONCLUSIONES

Los componentes de una topología de seguridad perimetral empleando una zona desmilitarizada, red interna, firewall-router e internet pueden ser abstraídos en elementos básicos, conservando la funcionalidad y operatividad de una red completa, posibilitando su estudio. La componente Intranet con un sistema operativo de amplio uso, corre el riesgo de infección por malware masivo, no obstante, los sistemas pertenecientes al componente DMZ, suelen ser objetivos de malware dirigido específicamente diseñado para transgredir particularidades.

La aplicación de tecnología de virtualización LXC y KVM según la finalidad e importancia de aislamiento en componentes, permite virtualizar redes con mayor cantidad de elementos salvaguardando los recursos físicos del servidor de virtualización. Para crear diferentes redes separadas e interconexión de máquinas virtuales, es suficiente con la utilización de switch virtuales y la correcta configuración de tarjetas de red.

El hipervisor Proxmox, facilita la interconexión de los componentes, permitiendo la configuración eficiente de la topología establecida. El empleo de una red de aislamiento completo con el uso de INetSim como servicio de emulación de protocolos comunes de Internet, permite un primer acercamiento sobre las funcionalidades de las muestras, no obstante, es necesaria la salida real a internet para mejorar resultados. Existe limitaciones en evaluación de elementos virtuales con herramientas externas; el software de monitoreo Zabbix , permite obtener gráficas de rendimiento, sin embargo, el cambio en la utilización de recursos debe de ser en extremo abrupto, para notar diferencias. Moloch permite la captura de paquetes de varias redes simultáneas, imposibilitado de comprender la carga útil de conexiones cifradas.

REFERENCIAS BIBLIOGRÁFICAS

Cross, T. (2014). StealthWatch & Point-of-Sale (POS) Malware. ***Lancope.*** https://www.slideshare.net/Lancope/retailwebinar

Enjoy Safer Tecnology. (2017). ***ESET Security Report Latinoamérica 2017.*** https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Enjoy Safer Tecnology. (2018). ***ESET Security Report Latinoamérica 2018.*** https://empresas.eset-la.com/archivos/novedades/69/ESET_security_report_LATAM2018-final.pdf

Iyer, A. S. (2005). Introduction to Enterprise Networks. https://www.it.iitb.ac.in/~sri/talks/Enterprise-05-Convergence.pdf

Kumar, R., & Charu, S. (2015). An Importance of Using Virtualization Technology in Cloud Computing. ***Global Journal of Computers & Technology, 1(2), 56-60.***

Sikorski, M., & Honig, A. (2012). Practical Malware Analysis. The Hans-On Guide to Dissectin Malicious Software. No Starch Press.

Zeltser, L. (2014). Automatización del análisis de malware estático con MASTIF. SANS™ Institute. https://digital-forensics.sans.org/blog/2013/05/07/mastiff-for-auto-static-malware-analysis