PREVENCIÓN, DETECCIÓN Y REDUCCIÓN DE RIESGOS DE ATAQUES POR ESCANEO DE PUERTOS USANDO TECNOLOGÍAS DE VIRTUALIZACIÓN

Karla Tandazo Jiménez, Miguel Rueda Salgado, Walter Fuertes Díaz, Diego Marcillo

ESPE, Ecuador, lita_ceci@hotmail.com
ESPE, Ecuador, miguerueda86@hotmail.com
ESPE, Ecuador, wmfuertes@espe.edu.ec
ESPE, Ecuador, dmarcillo@espe.edu.ec

RESUMEN

Las plataformas de virtualización son una gran alternativa para los escenarios de experimentación en redes IP. Estas proporcionan un espacio de trabajo controlable y estable, con la ventaja de reducir costos en la inversión y en la experimentación. Esta investigación evalúa de manera cuantitativa técnicas para escaneos de puertos para mitigar este tipo de ataques. Para lograrlo, se ha comprobado que las herramientas a ser usadas dispongan la capacidad de realizar este tipo de ataques, y también proporcionen medición para este experimento. Luego, se ha diseñado e implementado un laboratorio de equipos virtuales, el cual está en facultad de medir e identificar patrones que son propios de los ataques de escaneo de puertos. Para probar la eficacia de las opciones propuestas para mitigación, en la infraestructura virtualizada, se han tomado tiempos de retardo, cantidad de paquetes enviados, tiempo en completar las pruebas en los diferentes segmentos de red y la obtención de topologías, siendo este último realmente lo que pretende obtener este tipo de ataque. Finalmente, se ha logrado mitigar los ataques con un 96% de éxito, tomando en cuenta que la detección de patrones y el bloqueo del tráfico generado pueden afectar las comunicaciones del laboratorio de pruebas. Los tiempos de retardo son una métrica sensible a este tipo de solución, por lo tanto, filtrar e identificar un ataque implica un aumento en el tiempo que se necesita para realizar una comunicación exitosa entre un emisor y receptor.

Palabras Clave: Virtualización, Escaneo de Puertos, Firewall, Detección.

ABSTRACT

Virtualization platforms are a great choice for experimentation in IP networks. These platforms provides a controllable and stable scenario as well as reduce investment and experimentation cost. This research make an assessment of some port scanning techniques and options to reduce these potential threats. For carry out this, tools where verify to assure they provide needed functionality and measure capability. Later on, a specific virtual scenario had been designed and implemented for measure and identify patterns. Finally, for testing the efficacy of possible options to reduce this kind of attack, delay times, sent packages, time to complete the proposed attack and obtain network topologies were the metrics obtained after the experimentation. Finally, it had been tested some mitigation options with a 96% of success, knowing that patterns identification and blocking traffic could affect the communications of the experimentation lab. Delay Times is a sensible metric to this approaches, therefore, filter and identify an attack could increment the time needed to establish a successful communication.

KeyWords: Virtualization, Port Scanning, Firewall, Detection.

1. INTRODUCCIÓN

En la actualidad las organizaciones son informáticamente dependientes, los negocios se manejan en base a distintos tipos de software y bases de datos, en las cuales tienen información importante de clientes, proveedores, entre otros. Esta información tendrá que ser protegida interna y externamente, es decir, de los usuarios que conforman la empresa y de atacantes externos, respectivamente. El objetivo de esta protección es garantizar los recursos informáticos de la empresa para que no sufran ningún daño ni alteración[48].

Uno de los principales ataques es el escaneo de puertos [46], mediante el cual se pretende explorar una red en busca de potenciales puertas abiertas (puertos) y obtención de topologías. Para resolver este problema la comunidad científica ha desarrollado algunas investigaciones, tal es el caso, del trabajo propuesto por Fuertes en el cual se modificó la herramienta PSAD para detectar de manera más rápida y efectiva el ataque por escaneo de puertos. También, Carlton propone algunos escenarios para pruebas de diversas técnicas de hacking ético, en el cual se encuentran la cuantificación de escaneo de puertos en cloudcomputing.

El propósito de esta investigación es el diseño, implementación, experimentación y mitigación de técnicas de escaneo de puertos sobre una infraestructura virtualizada. Para el diseño de esta infraestructura se utilizó la normativa ISO 27004 y para la fase de experimentación, se tomó la metodología OSSTMM v3.0 para toma de muestras y cuantificación de los resultados; siendo estos el producto de la creación de soluciones que tienen por objetivo mitigar el escaneo de puertos, para lo cual, se realizó dichos experimentos con herramientas que permitan el ataque y la cuantificación de los mismos, como lo son NMAP y Wireshark respectivamente. Por esto, se ha logrado medir el envío de paquetes, consumo de ancho de banda, tiempos de retardo y adquirir topologías de la infraestructura relacionada con el trabajo.

En este contexto, se propuso y evaluó opciones para mitigación de escaneo de puertos, tomando en cuenta que todas las métricas mencionadas, como por ejemplo los tiempos de retardo, son sensibles a este tipo de soluciones, y son un factor crítico en las comunicaciones en redes IP. Por lo tanto, este trabajo presenta soluciones probadas en una infraestructura completamente virtualizada, sus ventajas y desventajas sobre las comunicaciones, el tráfico generado por la identificación de patrones y la cantidad de paquetes bloqueados.

El resto del artículo ha sido organizado como sigue: La sección 2 las metodologías utilizadas en este trabajo. La sección 3 describe el diseño, implementación y la línea base. La sección 4 presenta las soluciones propuestas, los resultados obtenidos después de la implementación de las mismas y la discusión respectiva del problema. La sección 5, muestra algunos trabajos relacionados y su influencia en este trabajo. Finalmente, la sección 6, se presentan las conclusiones, recomendaciones y trabajos a futuro.

2. METODOLOGÍA

2.1 Metodologías o Estándares de Seguridad Aceptados

- **ISO/IEC 27004**

Esta norma internacional proporciona una orientación sobre el desarrollo y uso de las medidas y la medición a fin de evaluar la eficacia de un sistema de gestión de la información aplicadas a la seguridad (SGSI-Sistemas de Gestión de la Seguridad de la Información) y los controles o grupos de controles, tal como se especifica en la norma ISO / IEC 27001[7]

Esto incluiría la política, la gestión de información de riesgos de seguridad, objetivos de control, controles, procesos y procedimientos, y apoyar el proceso de su revisión, lo que ayuda a determinar si alguno de los procesos o los controles del SGSI deben ser cambiados o mejorados. Hay que tener en cuenta que ninguna medida de control puede garantizar una seguridad total. La aplicación de este enfoque constituye un Programa de Medición de Seguridad de la Información.

El Programa de Medición de Seguridad de la Información será una ayuda a la administración en la identificación y evaluación de los procesos SGSI, cumplimiento de las normas, controles ineficaces, priorizando acciones asociadas con la mejora o cambio de estos procesos y controles.

- **OSSTMM**

Open Source Security Testing Methodology Manual[19], es una metodología desarrollada para test de Intrusión y verificación de hechos. Su objetivo en mira es medir como la seguridad funciona en una organización, basándose en métricas y hechos ineludibles que se estipulan al inicio de la metodología, al final de esta metodología se obtiene un informe en el cual se observa claramente lo que las normativas y políticas tomadas en una entidad realizan mas no lo que deberían realizar, es decir, es la situación actual de las políticas y normas de seguridad en la entidad.
Por lo cual, la importancia de probar un ambiente "seguro" es importante porque no todo funciona como está configurado y a veces, la gente no trabaja como esta entrenada, y con este tipo de herramientas podemos medir un ataque o una brecha de seguridad ya que se controla el ambiente mediante normativas para cualquier test de intrusión que se desee hacer en la infraestructura de nuestra entidad.

3 DISEÑO, IMPLEMENTACION Y LINEA BASE

3.1 Diseño del Escenario

En la Figura 1, se describe la conectividad del laboratorio y se muestran los equipos, puertos, VLANs y plataformas virtualizadas designadas en este trabajo, con el fin de reproducir y observar las tres 3 redes creadas que son la red interna, DMZ y red externa[1][31][36][42], con sus respectivos equipos y servicios a nivel macro.

El principal objetivo que persigue este diagrama es mostrar la parte física y su conectividad correspondiente en caso de ser necesario la reproducción del mismo, por lo tanto, para esta investigación, se ha utilizado un switch capa 3 con capacidad de VLAN's, ya que se desea agrupar lógicamente los puertos, para facilitar la administración de los equipos conectados en cada segmento de red.

También, se ha designado tres computadores, para virtualizar los diferentes equipos que componen este laboratorio, que cuentan con las siguientes características:

- **Equipo 1**
  - Procesador de 4 núcleos 2.4 GHz,, Intel i7
  - Memoria RAM DDR3 de 8 Gb
  - Espacio en disco de 500 Gb
  - tarjetas de Red (1 integrada a la PC y 2 tarjetas adicionales USB) todas de 1 Gigabit.
- **Equipo 2**
  - Procesador de 4 núcleos 2.4 GHz,, Intel i7
  - Memoria RAM DDR3 de 8 Gb
  - Espacio en disco de 500 Gb
  - 1 Tarjeta de Red de 1 Gigabit
- **Equipo 3**
  - Procesador de 2 núcleos 2.4 GHz,, Intel i5
  - Memoria RAM DDR3 de 4 Gb
  - Espacio en disco de 500 Gb
  - 1 Tarjeta de Red de 1 Gigabit
- **Switch**
  - Capa 3 Administrable
  - Capacidad de VLANS
  - 24 puertos 10/100 Megabit
  - puertos de 1 Gigabit
- **Router**
  - Máquina Virtual, configurada como Router
  - Firewall TMG

Adicionalmente, se usó un enrutador inalámbrico tipo N para acceder como un cliente externo, mediante VPN (Virtual Private Networks) al laboratorio [43].

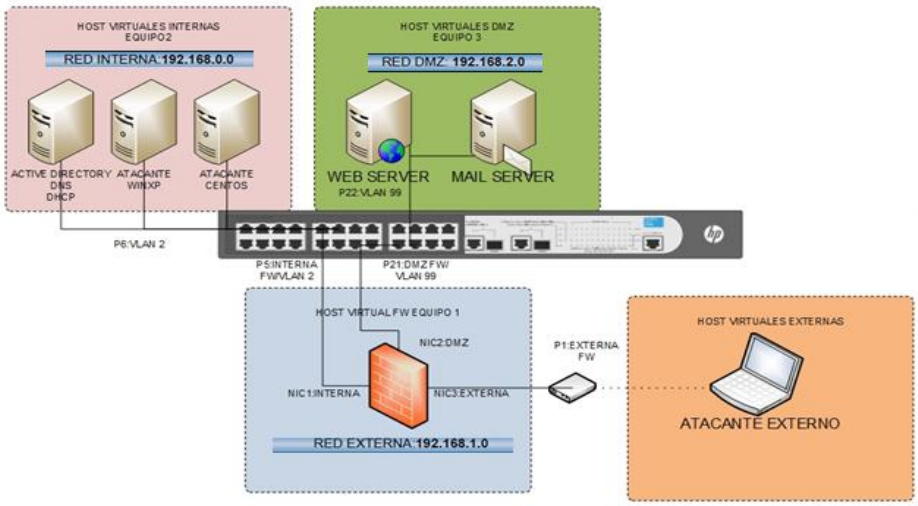

Figura 1. Diseño Físico del escenario virtual.

En la Figura 2, se encuentra el diagrama de servicios, el cual muestra cada equipo con nombre, dirección IP asignada y los servicios que presta para el laboratorio, puesto que el objetivo principal que persigue este diagrama, es dar un detalle de esta infraestructura, con el fin de que pueda administrar de manera eficaz cada parte de la infraestructura del laboratorio.

Además, con este diagrama se puede observar de manera clara, la configuración física de cada uno de los equipos utilizados en este laboratorio, ya que se observa la interface de red, IP asignada, y el software instalado en cada uno, y así se puede observar específicamente la estrategia que se ha propuesto en este laboratorio, los equipos dispuestos como atacantes, los servidores, servicios que se encuentran en esta infraestructura.

En resumen, este diagrama es la configuración inicial de este laboratorio, es la línea base de este trabajo, y es el producto final del diseño de esta infraestructura, que ha sido basada en estándares para su construcción

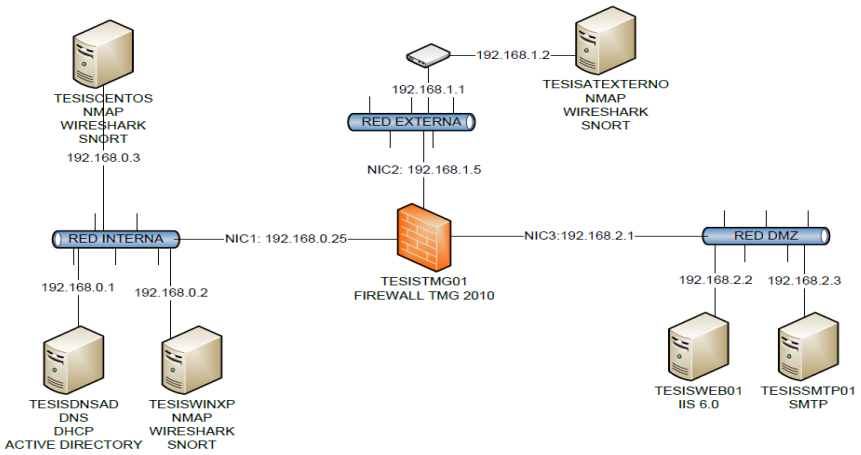

Figura 2. Diagrama de Servicios del escenario virtual.

3.2 Línea Base

Para la captura de tráfico de las redes externa, interna y DMZ para el experimento que se expone a continuación, se utilizó NMAP[28] para poder descubrir topologías de red y puertas abiertas que son los puertos, con lo cual se graficó la topología de la red Interna que fue la identificación de puertos y topología

de la red y Wireshark[22] cuya función es analizar el tipo de protocolos de red para realizar un filtrado de los mismos para la obtención de datos estadísticos de los ataques por red previo el uso de la metodología.
Los datos obtenidos por cada herramienta, han permitido, hacer una exploración de vulnerabilidades de la infraestructura planteada obteniendo métricas claras de la distribución de los elementos de red y sus puertos abiertos según cada ataque y segmento.
Según la herramienta NMAP los datos generales como tiempos de toma de cada muestra, se muestra en la tabla I y son los siguientes:

Tabla I: Resultados Muestra atacante Interno y Externo.

INTERNO	TCP	UDP	NULL	ACK
1	35.82	38.608	1059.84	110.07
2	36.28	36.074	954.78	112.78
3	35.53	38.401	1020.58	98.14
EXTERNO	**TCP**	**UDP**	**NULL**	**ACK**
1	78.65	85.040	1500.25	110.07
2	74.56	86.230	954.78	112.78
3	71.56	88.210	1020.58	98.14

Una característica importante en este tipo de ataque es el poder descubrir topologías de red y puertas abiertas que son los puertos, por lo cual el grafico de topología de la red Interna que fue obtenido por NMAP es un indicio de que el ataque fue satisfactorio.

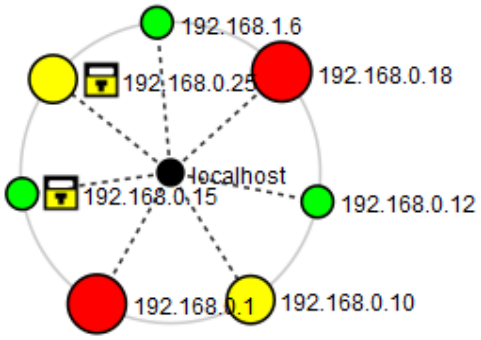

Figura 3: Topologia de red

La Figura 3, muestra que se ha logrado obtener la topología de la red, direcciones IP, datos de puertos y servicios corriendo en cada una de las computadoras graficadas, lo cual es una muestra clara y concreta de que la seguridad de la infraestructura ha sido vulnerada.

En la tabla II se muestran los consolidados, para el ataque TCP, en cuanto a paquetes, tiempos de retardo, tamaños y tiempos de transferencias, de las 3 muestras propuestas, mediante la herramienta Wireshark, lo cual es uno de los puntos más importantes de este trabajo, ya que determina el estado anterior en este trabajo y es indudablemente la pauta para el análisis de resultados.

Tabla II: Resultados de ataque escaneo TCP.

TCP	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25
Paquetes	64649,00	4812,00	3980,00	3518,00
Tiempo(ms)	4848,95	5827,27	3616,12	5828,39
paq/seg	11,03	0,83	1,10	0,60
Size(bytes)	114,10	84,39	64,53	761,05
Bytes	7376127,66	406103,93	256825,42	2677377,42
Bytes/s	1521,18	69,69	71,02	459,37

En la tabla III, se muestran los consolidados, para el ataque UDP, en cuanto a paquetes, tiempos de retardo, tamaños y tiempos de transferencias, de las 3 muestras propuestas, mediante la herramienta Wireshark.

Tabla III. Resultados de ataque Escaneo UDP

UDP	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25
Paquetes	54896,00	58987,00	48265,00	5026,00
Tiempo(ms)	5858,95	5827,27	3616,12	5851,96
paq/seg	9,37	10,12	13,35	0,86
Size(bytes)	111,20	85,53	78,89	140,35
Bytes	6104435,20	5045158,11	3807625,85	705399,10
Bytes/s	1041,90	865,78	1052,96	120,54

En la tabla IV, se muestran los consolidados, para el ataque Null Scan, en cuanto a paquetes, tiempos de retardo, tamaños y tiempos de transferencias, de las 3 muestras propuestas, de igual manera fueron tomados por Wireshark.

Tabla IV. Resultados de ataque NULL SCAN

NULL	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25
Paquetes	3341,000	3279,000	2258,000	46,000
Tiempo(ms)	1359,132	1359,132	1244,845	1331,168
paq/seg	2,458	2,413	1,814	0,035
Size(bytes)	137,370	135,001	71,232	202,217
Bytes	458953,170	442668,279	160841,856	9301,982
Bytes/s	337,681	325,699	129,206	6,988

En la tabla V, se muestran los consolidados, para el ataque ACK Scan, en cuanto a paquetes, tiempos de retardo, tamaños y tiempos de transferencias, de las 3 muestras propuestas, mediante la herramienta wireshark.

Tabla V. Resultados de ataque ACK SCAN

ACK	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25
Paquetes	10279	2632	2004	105
Tiempo(ms)	904,245	871,532	624,400	844,881
paq/seg	11,37	3,02	3,21	0,12
Size(bytes)	96	106.829	60.132	232.848
Bytes	990607,788	281173928	120504528	24449040
Bytes/s	1.095,508	322.620,315	192.992,518	28.937,850

En la Figura 4, se muestra el histograma de los paquetes enviados, como se observa en el gráfico, el ataque TCP es el ataque con mayor número de ataques enviados, por lo cual es un patrón claro para su mitigación.

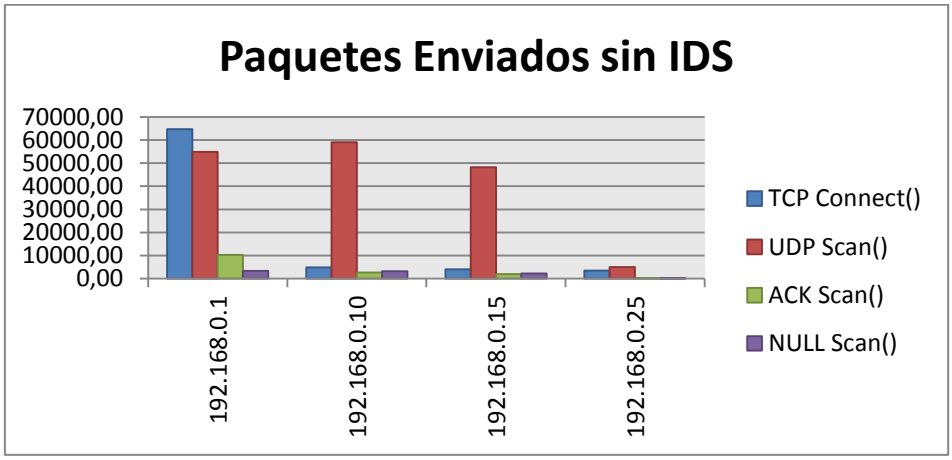

Figura 4: Datos Estadisticos por paquetes

Finalmente, la Figura 5, muestra el tiempo de retardo, es decir el tiempo que se toma en enviar el paquete entre emisor y receptor, esto se mide en milisegundos(ms) y es una métrica fundamental para la comparación de este trabajo.

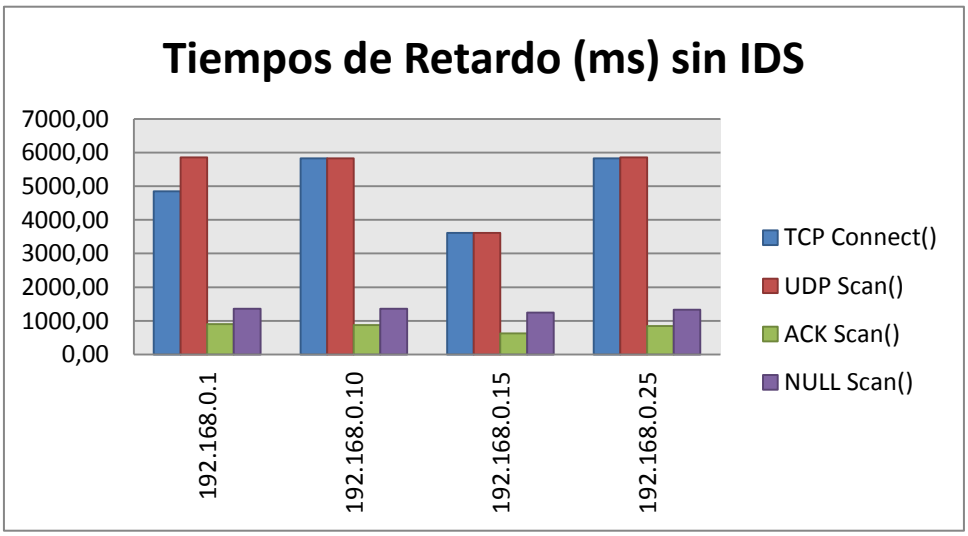

Figura 5:Datos Estadisticos por retrasos

4. RESULTADOS

4.1 Propuesta

Para evitar el ataque TCP, se propuso la siguiente regla, en el firewall, como se muestra en la Figura 6:

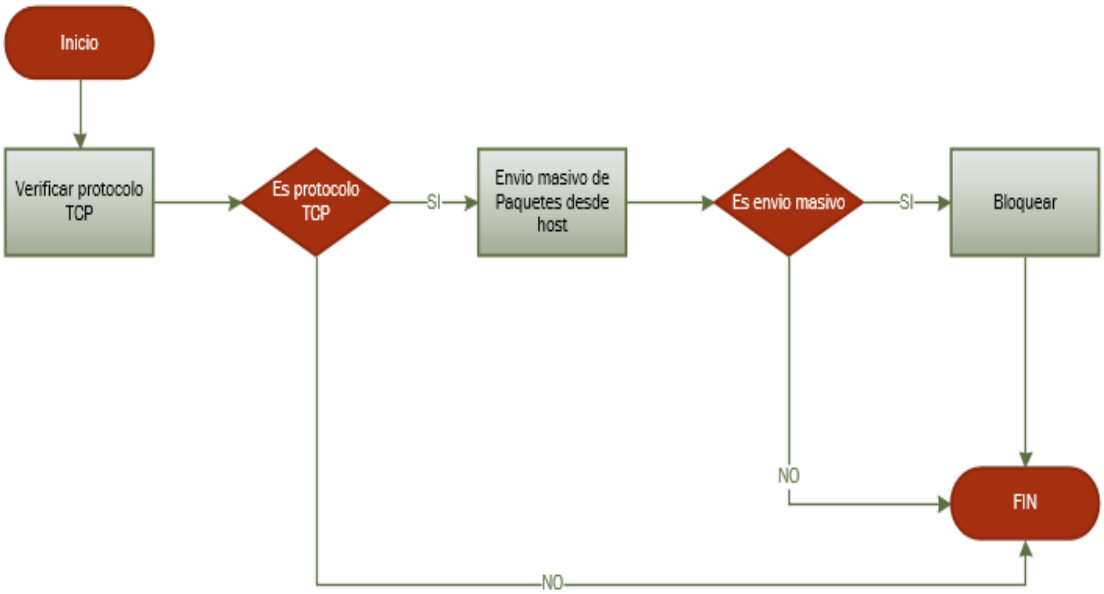

Figura 6: Regla Firewall TCP Scan

Para el ataque de UDP scan se ha propuesto la siguiente regla, como se ve en la Figura 7, ya que el patrón muestra un gran envío de paquetes UDP cada segundo:

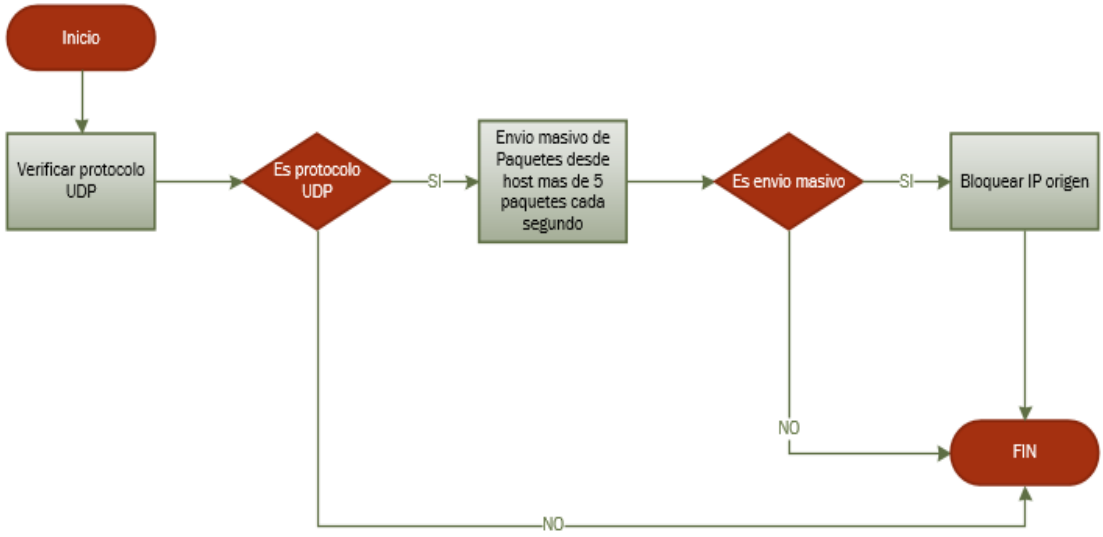

Figura 7: Regla Firewall UDP Scan

Para el ataque ACK Scan se propone la siguiente regla de firewall, ya que el patrón son las banderas RST, como se ve en la Figura 9:

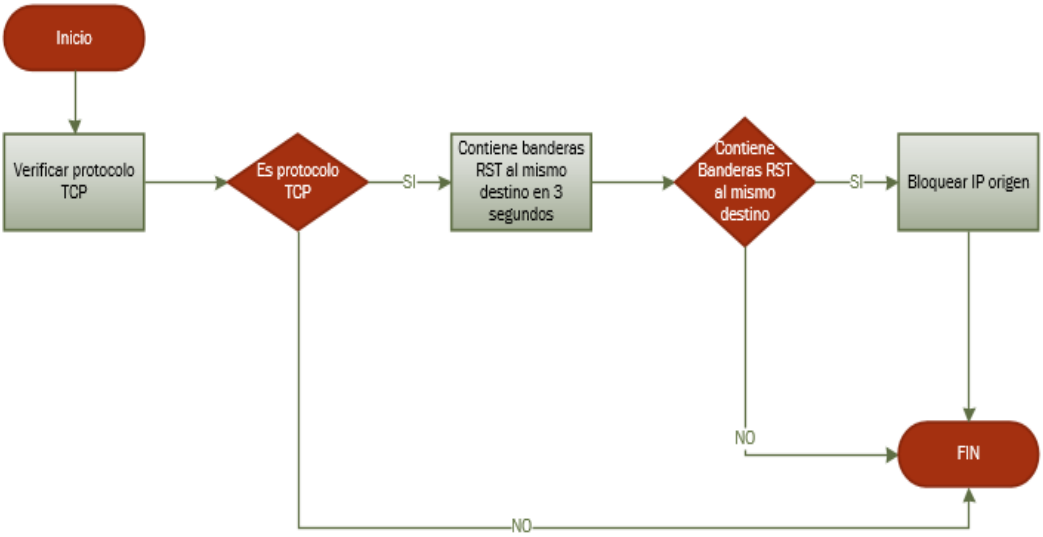

Figura 9: Regla Firewall ACK Scan

Para el ataque NULL Scan, es más complejo ya que se tiene que revisar las llamadas de múltiples banderas desde el mismo origen y enviadas al mismo tiempo, como se puede ver en la Figura 10:

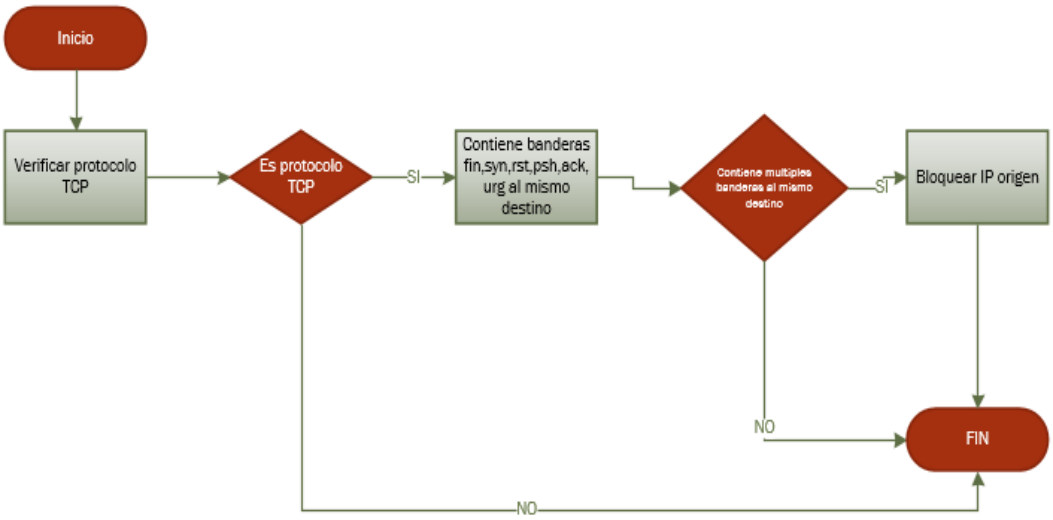

Fig.10: Regla Firewall NULL Scan

4.2 Evaluación de Resultados

La Figura 11, muestra el envío de paquetes después de la implementación del IDS y aplicando las reglas de Firewall para mitigar cada tipo de ataque, se puede observar que con relación a la línea base se han reducido el número de paquetes enviados en un 96% entre los diferentes ataques, lo cual muestra resultados positivos después de la fase de experimentación

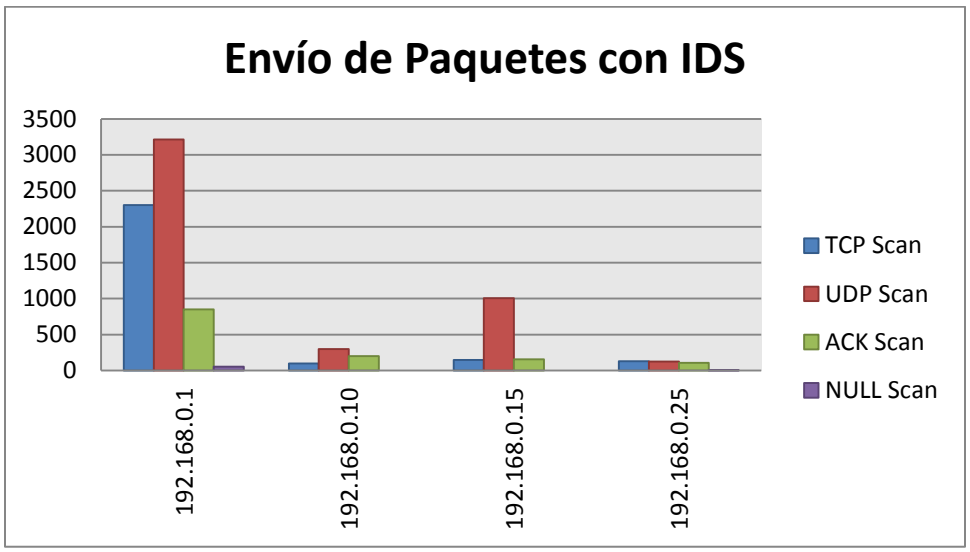

Figura 11: Datos Estadísticos envio con IDS

En cuanto a los tiempos de retardo como se ve en la Figura 12, hay un incremento del 40%, en consideración a la línea base, lo cual indica que los ataques están siendo bloqueados y toma más tiempo alcanzar a los diferentes equipos de la red, por esto, existe un retardo mayor en las comunicaciones del laboratorio.

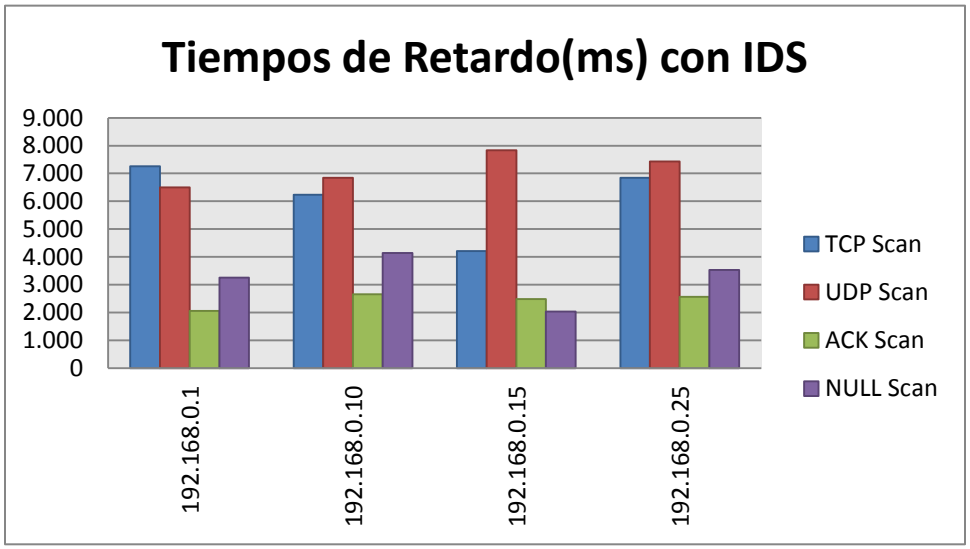

Figura 12: Datos Estadísticos por retrasos con IDS

4.3 Discusión

El laboratorio presenta una topología tipo estrella, ya que todos los equipos deben comunicarse por un punto en común en este caso el equipo designado como firewall, que es el equipo central en esta infraestructura. Por lo cual, sus principales ventajas son las siguientes:

- Si una computadora se desconecta o se rompe el cable solo queda fuera de la red aquel equipo.
- Posee un sistema que permite agregar nuevos equipos fácilmente.
- Reconfiguración Rápida.
- Fácil de prevenir daños y/o conflictos.
- Centralización de la red.

Sus principales desventajas son las siguientes:

- Si el equipo central falla, en nuestro caso el firewall, toda la red quedaría inhabilitada.
- El cableado debe ir del concentrador a cada equipo de la red.
- Es más costosa.

En este tipo de topología se logra administrar de manera simple la infraestructura por todas las ventajas enlistadas anteriormente, también propone un mayor grado de dificultad para restringir ataques, ya que las políticas corren en toda la red, por esto, se necesita minuciosidad al crear las diferentes reglas que norman la infraestructura, distinguiendo si es por equipos, segmentos o toda la red. Un hito en este trabajo es poder distinguir patrones ya que la mayoría de comunicaciones son vía el protocolo TCP/IP, por lo cual se ha encapsulado estos patrones en cada regla para poder mitigarla efectivamente, esto se observa, en los gráficos de las reglas del firewall, gracias a la implementación del IDS se pueden identificar estos patrones y bloquearlos, por lo cual se obtienen las siguientes mejoras por ataque, con respecto a los resultados obtenidos en la línea base.

En la Tabla VI se observa la cantidad de paquetes enviados haciendo comparación entre el mismo segmento de red cuando se realiza los diferentes tipos de ataques con IDS y sin IDS generando datos estadísticos que permiten cuantificar la mejora obtenida, con estos resultados se puede entender que los ataques propuestos han sido mitigados, aunque existe todavía un margen el cual puede ser mejorado, y en un tiempo lograr realmente evitarlo en un 100%.

Tabla VI Mejoras por Ataque

	PAQUETES ENVIADOS				PORCETAJE DE PAQUETES RECIBIDOS DESPUES DE REGLAS					
ATAQUE	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25	Promedio(%)	RESULTADO(%)
TCP SIN IDS	64649,00	4812,00	3980,00	3518,00	3,557672973	2,078137988	3,64321608	3,69528141	3,24357711	96,75642289
TCP CON IDS	2300	100	145	130						
UDP SIN IDS	54896,00	58987,00	48265,00	5026,00	5,854707082	0,508586638	2,080182327	2,467170712	2,72766169	97,27233831
UDP CON IDS	3214	300	1004	124						
ACK SIN IDS	10279	2632	2004	105	8,288744041	7,598784195	7,884231537	9,523809524	8,32389232	91,67610768
ACK CON IDS	852	200	158	10						
NULL SIN IDS	3341,000	3279,000	2258,000	46,000	1,61628255	0	0	4,347826087	1,49102716	98,50897284
NULL CON IDS	54	0	0	2						

5. TRABAJOS RELACIONADOS

Los resultados presentados anteriormente pueden ser comparados con otros. Aquí, los más relevantes encontrados en el transcurso de esta investigación:

En lo que refiere a escaneo de puertos, el trabajo presentado en [45] describe una mejora a un motor de libre distribución para detectar y bloquear escaneo de puertos mediante plataformas virtuales[41]. Dicho experimento describe comparativas de varios motores usando métricas como envió de paquetes y tiempos de retardo.

En este mismo contexto el autor de [42] presenta una comparación de varios escenarios virtuales para la experimentación de Firewall basados en Linux, usando tecnologías de virtualización como Xen Server y Virtualbox. Y en el trabajo [41] se comparan varias herramientas para virtualización, en donde se realizan pruebas intensivas CPU, memoria, acceso a disco duro, conectividad, creación de procesos y ataques de denegación de servicio.

De igual manera, en [40] se hace un estudio de la herramienta Wireshark y muestra varias maneras de realizar la captura de paquetes, filtrar y procesar los datos. Tambien, en [32] se habla sobre la herramienta NMAP y los diferentes ataques, entre ellos el escaneo de puertos, desde un punto de vista forense y de

hackeo ético, con sus principales ventajas, desventajas y posibles soluciones.

6. CONCLUSIONES Y TRABAJO FUTURO

Con este trabajo se demuestra la eficacia del Firewall TMG, ya que no se detectaron resultados en la red pública, sin embargo la mayoría de ataques son provocados por atacantes internos [47], por lo cual sí se utilizan reglas por defecto como son las que se han desarrollado para la implementación del laboratorio, es necesario un IDS, para poder controlar completamente el ataque. Una alternativa es utilizar un bloqueo interno o un bloqueo propuesto según los requerimientos del administrador de red, es importante recalcar que el IDS del firewall utilizado para este experimento posee la capacidad de aprender patrones de ataque y como se ha demostrado ha logrado bloquearlos.

Finalmente, como resultado del laboratorio se obtienen las siguientes mejoras en bloqueo de paquetes durante un ataque: TCP Scan tiene un 96,75%, en el caso de UDP Scan tiene 97.27%, ACK Scan del 91.67% y NULL Scan del 98.5%. De la misma manera, existe un aumento del 40% en tiempos de retardo, por lo tanto en las comunicaciones del laboratorio virtual se agrega alrededor de 2 segundos en establecer una transmisión entre emisor-receptor debido a la identificación y bloqueo de patrones.

Como trabajo a futuro se plantea la cuantificación de las técnicas de escaneo de puertos SYN Scan, Zombi Scan y RST Scan con el fin de identificar y crear más opciones para mitigación a los escaneos de puertos. Además, se propone utilizar firewall de distribución libre para la implementación de las soluciones propuestas y su cuantificación en esas plataformas.

7. REFERENCIAS BIBLIOGRÁFICAS

[1] CHESWICK, W. R.; BELLOVIN, S. M.; RUBIN, A. D. (2003). FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER, ADDISON-WESLEY PROFESSIONAL COMPUTING READING PAPERBACK, 2ND EDITION, ISBN 020163466X

[2] SECURITY: REPELLING THE WILY HACKER, 2ND ED. ADDISON-WESLEY NORTHCUTT, S. (2000). NETWORK INTRUSION DETECTION. AN ANALYST'S HANDBOOK. NEW RIDERS.

[3] SCAMBRAY, J.; MCCLURE, S.; KURTZ, G. (2001). HACKING EXPOSED: NETWORK SECURITY SECRETS AND SOLUTIONS, 2ND ED. OSBORNE-MCGRAW HILL.

[4] SILES PELAEZ, R. (2002). AN´ALISIS DE SEGURIDAD DE LA FAMILIA DE PROTOCOLOS TCP/IP Y SUS SERVICIOS ASOCIADOS.

[5] B.L HUTCHINGS, R.FRANKLIN, D. CARVER, "ASSISTING NETWORK INTRUSION DETECTION WITH RECONFIGURABLE HARDWARE",2002

[6] 27000.ORG. (S.F.). HTTP://WWW.27000.ORG/. OBTENIDO DE HTTP://WWW.27000.ORG/: HTTP://WWW.27000.ORG/ISO-27004.HTM

[7] CORLETTI, A. (MARZO DE 2007). WWW.CRIPTORED.UPM.ES. OBTENIDO DE WWW.CRIPTORED.UPM.ES: HTTP://WWW.CRIPTORED.UPM.ES/GUIATEORIA/GT_M292J.HTM

[8] DAEMON, M. (09 DE 06 DE 2006). WWW.ESPE.EDU.EC.

[9] DRAGONJAR. (S.F.). WWW.DRAGONJAR.ORG. OBTENIDO DE WWW.DRAGONJAR.ORG: HTTP://WWW.DRAGONJAR.ORG/OSSTMM-MANUAL-DE-LA-METODOLOGIA-ABIERTA-DE-TESTEO-DE-SEGURIDAD.XHTML

[10] ECUALUG. (S.F.). OBTENIDO DE VIRTUALIZACIÓN: HTTP://WWW.ECUALUG.ORG/2012/02/09/BLOG/EPE/CURIOSIDADES_DE_KVM_KSM

[11] FERNANDEZ, D. (04 DE 2008). WWW.REDIRIS.ES. OBTENIDO DE HTTP://WWW.REDIRIS.ES/DIFUSION/PUBLICACIONES/BOLETIN/82-83/PONENCIA1.4A.PDF

[12] FUENTE, I. R. (2011). CERTIFICACIONES URUGUAY. OBTENIDO DE CERTIFICACIONES URUGUAY: HTTP://WWW.CERT.UY/HISTORICO/PDF/CERTIFICACIONESPROFESIONALESENSEGURIDADDELAINFORMACIONL.PDF

[13] ISECOM. (S.F.). WWW.ISECOM.ORG. OBTENIDO DE WWW.ISECOM.ORG: HTTP://WWW.ISECOM.ORG/MIRROR/OSSTMM.3.PDF

[14] LINUX PARA TODOS. (S.F.). OBTENIDO DE HTTP://WWW.LINUXPARATODOS.NET/WEB/COMUNIDAD/BASE-DE-CONOCIMIENTO/-/WIKI/BASE+DE+CONOCIMIENTO/KERNEL+BASED+VIRTUAL+MACHINE+%28KVM%29;JSESSIONID=4670265DBC57B6E1FD21C048854E5209#SECTION-KERNEL+BASED+VIRTUAL+MACHINE+%28KVM%29-CARACTER%C3%ADSTICAS+KVM

[15] LLERENA, M., & SAA, J. D. (20 DE 04 DE 2006). ESPE REPOSITORIO.

[16] MARQUEZ, O. (25 DE 09 DE 2008). DIRECTOR DE LA DIVISIÓN DE SOLUCIONES SERVIDORES Y ALMACENAMIENTO DE HP. (CARACASDIGITAL, ENTREVISTADOR)

[17] NMAP. (S.F.). HTTP://NMAP.ORG/. OBTENIDO DE HTTP://NMAP.ORG/: HTTP://NMAP.ORG/MAN/ES/

[18] OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM). (2010). OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM). OBTENIDO DE OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM): HTTP://WWW.ISECOM.ORG/RESEARCH/OSSTMM.HTML

[19] SEGURIDAD Y REDES. (S.F.). OBTENIDO DE HTTP://SEGURIDADYREDES.NIREBLOG.COM/POST/2008/03/24/ANALISIS-DE-RED-CON-WIRESHARK-FILTROS-DE-CAPTURA-Y-VISUALIZACIAN

[20] VINCOSOFT. (S.F.). HTTP://WWW.VICOMSOFT.COM/LEARNING-CENTER/PPPOE/. OBTENIDO DE HTTP://WWW.VICOMSOFT.COM/LEARNING-CENTER/PPPOE/.

[21] WIRESHARK. (S.F.). OBTENIDO DE HTTP://SEGURIDADYREDES.NIREBLOG.COM/POST/2010/03/24/WIRESHARK-TSHARK-CAPTURANDO-IMPRESIONES-EN-RED

[22] DAEMON, M. (09 DE 06 DE 2006). WWW.ESPE.EDU.EC.

[23] ECUALUG. (S.F.). OBTENIDO DE VIRTUALIZACIÓN: HTTP://WWW.ECUALUG.ORG/2012/02/09/BLOG/EPE/CURIOSIDADESDE_KVM_KSM

[24] FERNANDEZ, D. (04 DE 2008). WWW.REDIRIS.ES. OBTENIDO DE HTTP://WWW.REDIRIS.ES/DIFUSION/PUBLICACIONES/BOLETIN/82-83/PONENCIA1.4A.PDF

[25] FUENTE, I. R. (2011). CERTIFICACIONES URUGUAY. OBTENIDO DE CERTIFICACIONES URUGUAY: HTTP://WWW.CERT.UY/HISTORICO/PDF/CERTIFICACIONESPROFESIONALESENSEGURIDADDELAINFORMACIONL.PDF

[26] ISECOM. (S.F.). WWW.ISECOM.ORG. OBTENIDO DE WWW.ISECOM.ORG: HTTP://WWW.ISECOM.ORG/MIRROR/OSSTMM.3.PDF

[27] NMAP. (S.F.). HTTP://NMAP.ORG/. OBTENIDO DE HTTP://NMAP.ORG/: HTTP://NMAP.ORG/MAN/ES/

[28] ACM SIGCOMM INTERNET MEASUREMENT CONFERENCE, ASSOCIATION FOR COMPUTING MACHINERY, & USENIX ASSOCIATION. (2004). IMC 2004: PROCEEDINGS OF THE 2004 ACM SIGCOMM INTERNET MEASUREMENT CONFERENCE, TAORMINA, SICILY, ITALY, OCTOBER 25-27, 2004. NEW YORK, N.Y: ACM PRESS.

[29] ACM WORKSHOP ON EXPERIMENTAL COMPUTER SCIENCE. (2007). PROCEEDINGS OF THE 2007 WORKSHOP ON EXPERIMENTAL COMPUTER SCIENCE: JUNE 13-14, 2007, SAN DIEGO, CALIFORNIA. --. ACM PRESS.

[30] AUSTRALASIAN TELECOMMUNICATION NETWORKS AND APPLICATIONS CONFERENCE, I. OF E. AND E. E. (2009). 2009 AUSTRALASIAN TELECOMMUNICATION NETWORKS AND APPLICATIONS CONFERENCE ATNAC 2009: PROCEEDINGS : 10-11 NOVEMBER 2009, CANBERRA, AUSTRALIA. RETRIEVED MAY 23, 2013, FROM HTTP://IEEEXPLORE.IEEE.ORG/SERVLET/OPAC?PUNUMBER=5457370

[31] CARLTON, G. H., & ZHOU, H. (2011). A SURVEY OF CLOUD COMPUTING CHALLENGES FROM A DIGITAL FORENSICS PERSPECTIVE. INTERNATIONAL JOURNAL OF INTERDISCIPLINARY TELECOMMUNICATIONS AND NETWORKING, 3(4), 1–16. DOI:10.4018/JITN.2011100101

[32] FOROUZAN, B. A. (2003). TCP/IP PROTOCOL SUITE (2ND ED.). BOSTON: MCGRAW-HILL.

[33] GÁLVEZ MOZO, A. M. (2006). SOCIABILIDAD EN PANTALLA: UN ESTUDIO DE LA INTERACCIÓN EN LOS ENTORNOS VIRTUALES. BARCELONA: EDITORIAL UOC.

[34] GARFINKEL, S. (2002). WEB SECURITY, PRIVACY AND COMMERCE (2ND ED. EXPANDED & UPDATED.). CAMBRIDGE, MASS: O'REILLY.

[35] HARRISON, J. (2010). MICROSOFT FOREFRONT THREAT MANAGEMENT GATEWAY (TMG): ADMINISTRATOR'S COMPANION. REDMOND, WASH: MICROSOFT PRESS.

[36] INTERNATIONAL CONFERENCE ON INNOVATIONS IN INFORMATION TECHNOLOGY. (2008). INNOVATIONS '07 4TH INTERNATIONAL CONFERENCE ON INNOVATIONS IN INFORMATION TECHNOLOGY: CONFERENCE PROCEEDINGS, DUBAI, NOVEMBER 18-20, 2007. IEEE.

[37] LYON, G. F. (2008). NMAP NETWORK SCANNING: OFFICIAL NMAP PROJECT GUIDE TO NETWORK DISCOVERY AND SECURITY SCANNING (1ST ED.). SUNNYVALE, CA: INSECURE.COM, LLC.

[38] NORTH AMERICAN FUZZY INFORMATION PROCESSING SOCIETY. (2000). PEACHFUZZ 2000: 19TH INTERNATIONAL CONFERENCE OF THE NORTH AMERICAN FUZZY INFORMATION PROCESSING SOCIETY--NAFIPS: ATLANTA, GEORGIA, USA, JULY 13-15, 2000. PISCATAWAY, NJ: IEEE.

[39] OREBAUGH, A. (2007). WIRESHARK & ETHEREAL: NETWORK PROTOCOL ANALYZER TOOLKIT. ROCKLAND, MA: SYNGRESS.

[40] QUÉTIER, B., NERI, V., & CAPPELLO, F. (2006). SCALABILITY COMPARISON OF FOUR HOST VIRTUALIZATION TOOLS. JOURNAL OF GRID COMPUTING, 5(1), 83–98. DOI:10.1007/S10723-006-9052-6

[41] RASH, M. (2007). LINUX FIREWALLS: ATTACK DETECTION AND RESPONSE WITH IPTABLES, PSAD, AND FWSNORT. SAN FRANCISCO: NO STARCH PRESS.

[42] SCOTT, C. (1999). VIRTUAL PRIVATE NETWORKS (2ND ED.). BEIJING [CHINA] ; SEBASTOPOL, CA: O'REILLY.

[43] SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE, I. C. S. (2005). 46TH ANNUAL IEEE SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE FOCS 2005: 23-25 OCTOBER, 2005, PITTSBURGH, PENNSYLVANIA, USA. RETRIEVED MAY 23, 2013, FROM HTTP://IEEEXPLORE.IEEE.ORG/SERVLET/OPAC?PUNUMBER=10244

[44] W FUERTES, P ZAMBRANO, S MARCO. (2011). ALTERNATIVE ENGINE TO DETECT AND BLOCK PORT SCAN ATTACKS USING VIRTUAL NETWORK ENVIRONMENTS. QUITO.

[45] OWASP (S.F) OBTENIDO DE HTTPS://WWW.OWASP.ORG/INDEX.PHP/CATEGORY:ATTACK

[46] CERT ORG OBTENIDO DE HTTP://WWW.CERT.ORG/

[47] KOTLER, P (1974), DIRECCIÓN DE MERCADOTECNIA, ANÁLISIS, PLANEACIÓN Y CONTROL, MÉXICO DF