ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

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

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR: KARLA TANDAZO JIMENEZ Y MIGUEL ANGEL RUEDA SALGADO

Sangolquí, Agosto del 2013

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Nosotros, **KARLA CECIBEL TANDAZO JIMENEZ** y **MIGUEL ANGEL RUEDA SALGADO**

Autorizamos a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución, del trabajo "**PREVENCIÓN, DETECCIÓN Y REDUCCIÓN DE RIESGOS DE ATAQUES POR ESCANEO DE PUERTOS USANDO TECNOLOGÍAS DE VIRTUALIZACIÓN.**", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Agosto del 2013

_____	_____
Karla Cecibel Tandazo Jiménez	Miguel Ángel Rueda Salgado

DECLARACIÓN

Nosotros, Karla Cecibel Tandazo Jimenez y Miguel Ángel Rueda Salgado, declaramos que el presente trabajo es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación personal y que hemos consultado las referencias bibliográficas que se incluyen en el documento.
La Escuela Politécnica del Ejército puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual por su reglamento y por la normativa institucional vigente.

Sangolquí, Agosto de 2013

_____ _____

Karla Cecibel Tandazo Jiménez Miguel Ángel Rueda Salgado

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por la Srta. KARLA CECIBEL TANDAZO JIMENEZ y el Sr. MIGUEL ANGEL RUEDA SALGADO como requerimiento parcial a la obtención del título de INGENIEROS EN SISTEMAS E INFORMÁTICA

Sangolquí, Agosto del 2013

_____	_____
DR. WALTER FUERTES	ING.DIEGO MARCILLO
DIRECTOR DE TESIS	CODIRECTOR DE TESIS

DEDICATORIA

A mis padres Sixto Tandazo y Beatriz Jiménez, que me han brindado su apoyo en cada momento de mi vida, por enseñarme a luchar y seguir mis ideales. Gracias a ustedes he podido llegar a cumplir esta meta.

Karla Tandazo

AGRADECIMIENTO

"*Es tan grande el placer que se experimenta al encontrar un hombre agradecido que vale la pena arriesgarse a no ser un ingrato"* Lucio Anneo Séneca

Expreso mi más sincero agradecimiento a todos quienes hicieron posible la consecución de este trabajo. A ti querido amigo Mike que realizaste conmigo este trabajo de tesis, aportando tu tiempo, conocimiento y poniendo siempre tu buena voluntad para la terminación del mismo.

Un agradecimiento especial a nuestras familias, quienes con su preocupación y entrega han hecho que nuestros esfuerzos rindieran sus frutos. Por la confianza brindada y el incondicional apoyo.

Gracias

Karla Tandazo

DEDICATORIA

A mi familia y a mis padres, que me acompañan todos los días de mi vida, que me dan esa energía necesaria para perseguir y alcanzar mis metas.

Miguel Ángel Rueda

AGRADECIMIENTO

A mi amada familia, a mis padres que me han apoyado incondicionalmente en cada paso de mi vida, a mi querida Karlita por ser un pilar y una bendición en el transcurso de este trabajo.
Un agradecimiento especial al Ing. Walter Fuertes Díaz PhD. por brindarnos una invalorable ayuda y esta oportunidad que se ha transformado en un paso importantísimo en nuestras vidas.

Muchísimas gracias a todos mis amigos por el aliento y a mí querida universidad que me ha brindado conocimiento, amistades y momentos inolvidables.

Gracias

Miguel Ángel Rueda

Índice de Contenidos

Resumen 1
CAPÍTULO 1: INTRODUCCIÓN 2
1.1- Tema 2
1.2- Introducción 2
1.3- Problema de Investigación 3
1.3.3- Preguntas de investigación 3
1.3.4- Planteamiento de problema 4
1.4- Justificación 4
1.5.- Objetivos 5
1.5.1- Objetivo general 5
1.5.2- Objetivos específicos 5
1.5- Alcance 6
CAPÍTULO 2: MARCO TEÓRICO 7
2.1- Conceptos sobre conexiones TCP 7
2.2- Estableciendo conexiones: sockets, puertos e IP's 7
2.3- Desconexión TCP 8
2.4- Conceptos de virtualización 9
2.4.1-Generalidades 9
2.4.2-Virtualización de servidores 10
2.4.3-Virtualización a nivel de Hardware 10
2.4.4-Virtualización a nivel del sistema operativo 11
2.4.5-Aplicaciones 13
2.4.6-Sistema operativo 13
2.4.7-Aplicaciones para virtualización 14
2.5- Técnicas de escaneo 14
2.5.1-ACK Scan 14
2.5.2-NULL Scan 15
2.5.4- Xmas Scan 16
2.5.5- SYN/ACK Scan 16
2.5.6- RPC Scan 16
2.5.7- Zombie Scan 17

2.6- Herramientas de seguridad y análisis de vulnerabilidades 18
2.6.1- NMAP (Mapeador de redes) 18
2.6.2- Características NMAP 19
2.6.3- Wireshark 20
2.7- Metodologías o estándares de seguridad aceptados 21
2.7.1- ISO/IEC 27004 21
2.7.2- OSSTMM 22
CAPÍTULO 3: DISEÑO Y CONSTRUCCIÓN DE LABORATORIO DE PRUEBAS 23
3.1- Introducción 23
3.2- Diseño de la arquitectura 23
3.2.1- Diagrama Físico 27
3.2.2- Diseño Lógico 30
3.2.3- Diseño de los servicios de la red 32
3.3- Configuración de la plataforma de experimentación, Línea Base 33
CAPÍTULO 4:MITIGAR ATAQUES POR ESCANEO DE PUERTOS 36
4.1- Introducción 36
4.2- Toma de datos 36
4.3- Procesamiento estadístico de datos (Línea Base) 42
4.4- Algoritmo para detectar, controlar y mitigar ataques por escaneo de puertos. 44
4.5- Evaluación de resultados 49
4.5.1- Discusión 51
CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES 54

Listado de Gráficos

Capítulo 2 MARCO TEÓRICO

Fig 2.1: Establecimiento de conexión 12
Fig 2.2: Finalización de conexión 12
Fig 2.3: Virtualización servidores 14
Fig 2.4: Virtualización Hardware 15
Fig 2.5: Virtualización por Software 17
Fig 2.6: Aplicaciones para virtualizar 19
Fig 2.7: ACK Scan 20
Fig 2.8: Null Scan 20

Capítulo 3 DISEÑO Y CONSTRUCCIÓN DE LABORATORIO DE PRUEBAS

Fig 3.1: Diagrama Físico 30
Fig 3.2: Diagrama Lógico 31
Fig 3.3: Diagrama de Servicios 32
Fig 3.4: Reglas de Firewall 33
Fig 3.5: Regla Allow Web Access s 43
Fig 3.6: Regla DNS Server 44

Capítulo 4 PRUEBAS Y ANÁLISIS DE RESULTADOS ATAQUE DE ESCANEO DE PUERTOS

Fig 4.1: Topología de red 52
Fig 4.2: Datos estadísticos Red interna 43
Fig 4.3: Datos estadísticos Red externa 44
Fig 4.4: Datos estadísticos por paquetes 44
Fig 4.5: Datos estadísticos por retrasos 45
Fig 4.6: Regla Firewall TCP Scan 54
Fig 4.7: Regla Firewall UDP Scan 55
Fig 4.8: Regla Firewall ACK Scan 55
Fig 4.9: Regla Firewall NULL Scan 56
Fig 4.10: Comparación estadística de datos por paquetes 58
Fig 4.11: Comparación estadística de datos por tiempos 59

Listado de Tablas

Tabla 4.1: Resultados Muestra atacante Interno y Externo 50
Tabla 4.2: Resultados de ataque escaneo TCP…… 51
Tabla 4.3: Resultados de ataque escaneo UDP 52
Tabla 4.4: Resultados de ataque NULL Scan. 53
Tabla 4.5. Resultados de ataque ACK Scan..... .53
Tabla 4.6: Resultados de ataque escaneo TCP. 54
Tabla 4.7: Resultados de ataque escaneo UDP. 54
Tabla 4.8: Resultados de ataque NULL Scan. 55
Tabla 4.9: Resultados de ataque ACK Scan..... 55
Tabla 4.10: Resultados TCP Scan con IDS. 61
Tabla 4.11: Resultados UDP Scan con IDS. 61
Tabla 4.12: Resultados ACK Scan con IDS..... .62
Tabla 4.13: Resultados TCP Scan con IDS. 62
Tabla 4.14: Mejoras por ataque..... 66

Listado de Anexos

Anexos A

Anexos Fig.A.1: Vmware8 .. ……. ……..…..i

Anexos Fig.A. 2: VMware8 wizard. i

Anexos Fig.A. 3:VMware8 wizard. Tipo de Instalación..... ii

Anexos Fig.A. 4: VMware8 wizard. Ubicación de instalación. ii

Anexos Fig.A. 5: VMware8 wizard. Colaboración VMware..... .iii

Anexos Fig.A. 6: VMware8. Wizard shortcuts. iii

Anexos Fig.A. 7: VMware8 wizard iv

Anexos Fig.A. 8: VMware8. Instalación. iv

Anexos Fig.A. 9: VMware8. Product Key. v

Anexos Fig.A.10: VMware8. License Agreement v

Anexos Fig.A.11: VMware8. Actualizaciones vi

Anexos B

Anexos Fig.B.1: Wizard instalación TMG vi

Anexos Fig.B.2: TMG2010 License Terms. vii

Anexos Fig.B.3: Wizard instalación TMG vii

Anexos Fig.B.4: Wizard empezar instalación TMG. viii

Anexos Fig.B.5: TMG2010. viii

Anexos Fig.B. 6: TMG2010 License Terms ix

Anexos Fig.B.7: TMG2010 Product key ix

Anexos Fig.B.8: TMG2010 Internal Network. x

Anexos Fig.B. 9: TMG2010 Internal Network. x

Anexos Fig.B. 10: TMG2010 componentes xi

Anexos Fig.B.11: TMG2010 Instalación completa. xi

Anexos Fig.B.12: TMG2010 Configuración de la red. xii

Anexos Fig.B.13: TMG2010 Elegir modelo de red. xii

Anexos Fig.B.14: TMG2010 Red interna. xiii

Anexos Fig.B.15: TMG2010 Configuración de la red. Externa. xiii

Anexos Fig.B.16: TMG2010 Configuración DMZ. xiv

Anexos Fig.B.17: TMG2010 Terminar configuración. xiv

Anexos Fig.B.18: TMG2010 Configuración sistema. xv

Anexos Fig.B.19: TMG2010 Configuración dominio xv

Anexos Fig.B.20: TMG2010 Políticas. xvi

Anexos Fig.B.21: TMG2010 Definición de políticas..... xvi
Anexos Fig.B.22: TMG2010 Configuración. xvii
Anexos Fig.B.22: TMG2010 Configuración. xvii
Anexos Fig.B.24: TMG2010 Manejo de usuarios xviii
Anexos Fig.B.25: TMG2010 Configuración de contenidos xviii
Anexos Fig.B.26: TMG2010 Configuración tráfico Https xix
Anexos Fig.B.27: TMG2010 Configuración cache. xix
Anexos Fig.B.28: TMG2010 Configuración completa..... xx
ANEXO C
Anexos Fig.C.1: VMware Creación máquinas virtuales. xx
Anexos Fig.C.2: VMware Wizard de configuración. xxi
Anexos Fig.C.3: VMware Origen de instalación. xxi
Anexos Fig.C.4: VMware Instalador. xxii
Anexos Fig.C.5: VMware Confirmar origen de instalación. xxii
Anexos Fig.C.6: VMware Selección de nombre de VMachine xxiii
Anexos Fig.C.7: VMware Asignación de disco. xxiii
Anexos Fig.C.8: VMware Configuración de VM. xxiv
Anexos Fig.C.9: Instalación del SO. xxiv
ANEXO D
Anexos Fig.D.1: Active Directory y DHCP..... xxv
Anexos Fig.D.2: Active Directory y DHCP..... xxv
Anexos Fig.D.3: Active Directory y DHCP..... xxvi
Anexos Fig.D.4: Active Directory y DHCP..... xxvi
Anexos Fig.D.5: Active Directory y DHCP..... xxvii
Anexos Fig.D.6: Active Directory y DHCP..... xxvii
Anexos Fig.D.7: Active Directory y DHCP..... xxviii
Anexos Fig.D.8: Active Directory y DHCP..... xxviii
Anexos Fig.D.9: Active Directory y DHCP..... xxix
Anexos Fig.D.10: Configurar Servidor DNS. xxix
Anexos Fig.D.11: Configurar Servidor DNS. xxx
Anexos Fig.D.12: Configurar Servidor DNS. xxx
Anexos Fig.D.13: Configurar Servidor DNS. xxxi
Anexos Fig.D.14: Configurar Servidor DNS. xxxi
Anexos Fig.D.15: Configurar Servidor DNS. xxxii

Anexos Fig.D.16: Configurar Servidor DNS. xxxii
Anexos Fig.D.17: Configurar Servidor DNS. xxxiii
Anexos Fig.D.18: Configurar Servidor DNS. xxxiii
ANEXO E
Anexos Fig.E.1: Servicios configurados en equipo. xxxiv
Anexos Fig.E.2: Instalación del cliente TMG 2010..... xxxiv
Anexos Fig.E.3: Instalación del cliente TMG 2010..... xxxv
Anexos Fig.E.4: Instalación del cliente TMG 2010..... xxxv
Anexos Fig.E.5: Instalación del cliente TMG 2010..... xxxvi
Anexos Fig.E.6: Instalación del cliente TMG 2010..... xxxvi
Anexos Fig.E.7: Instalación del cliente TMG 2010..... xxxvii
Anexos Fig.E.8: Instalación del cliente TMG 2010..... xxxvii
Anexos Fig.E.9: Instalación del cliente TMG 2010..... xxxviii
Anexos Fig.E.10: Instalación del cliente TMG 2010..... xxxviii
Anexos Fig.E.11: Instalación del cliente TMG 2010..... xxxix
ANEXO F
Anexos Fig.F.1: Configuración del cliente TMG 2010. xxxix
Anexos Fig.F.2: Configuración del cliente TMG 2010. xl
ANEXO G
Anexos Fig.G.1: Instalación NMAP..... xl
Anexos Fig.G.2: Instalación NMAP..... xli
Anexos Fig.G.3: Instalación NMAP..... xli
Anexos Fig.G.4: Instalación NMAP..... xlii
Anexos Fig.G.5: Instalación NMAP..... xlii
Anexos Fig.G.6: Instalación NMAP..... xliii
Anexos Fig.G.7: Instalación NMAP..... xliii
Anexos Fig.G.8: Instalación NMAP..... xliv
ANEXO H
Anexos Fig.H.1: Instalación Wireshark. xliv
Anexos Fig.H. 2: Instalación Wireshark xlv
Anexos Fig.H. 3: Instalación Wireshark xlv
Anexos Fig.H.4: Instalación Wireshark. xlvi
Anexos Fig.H.5: Instalación Wireshark. xlvi
Anexos Fig.H.6: Instalación Wireshark. xlvii

Anexos Fig.H.7: Instalación Wireshark. xlvii
Anexos Fig.H.8: Instalación Wireshark. xlviii
Anexos Fig.H.9: Instalación Wireshark xlviii
Anexos Fig.H.10: Instalación Wireshark. xlix

Nomenclatura utilizada

ACK: Acuse de recibo

DMZ: Zona desmilitarizada

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name Server

FTP: File Transfer Protocol

GPL: General Public License

HTTP: HyperText Transfer Protocol

ICMP: Internet Control Message Protocol

IDS: Intrusion Detection System

IEC: Comisión Electrotécnica Internacional

IP: Internet Protocol

ISO: International Organization for Standardization

ISP: Proveedor de Servicios de Internet

OSSTMM: Open Source Security Testing Methodology Manual

PPPoE: Point-to-point protocol over Ethernet

RPC: RemoteProcedureCall

SGSI: Sistema de Gestión de la Seguridad de la Información

SMTP: Simple Mail Transfer Protocol

SYN: Synchronization Character

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

VLAN: Virtual Local Area Networks

VPN: Virtual Private Network

AD: Active Directory

Resumen

El presente proyecto, describe la 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. Los resultados obtenidos han sido el producto de la experimentación con soluciones propuestas en este trabajo, 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 resultados, como lo son NMAP y Wireshark respectivamente. Por esto, se ha logrado medir el envío de paquetes, medición de banda ancha, tiempos de retardo y adquirir topologías de la infraestructura.

Finalmente, se ha logrado mitigar los ataques con un porcentaje del 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. Es por esto, que 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. Todos estos aspectos han sido debidamente analizados en este trabajo y han sido probados en su totalidad en un laboratorio de máquinas virtuales.

CAPÍTULO 1: INTRODUCCIÓN

1.1- Tema

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

1.2- Introducción

En la actualidad, la mayoría de organizaciones es informáticamente dependiente, los negocios se manejan con base en 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.

El uso de computadoras, transacciones bancarias, Internet, cajeros automáticos, entre otros, generan registros con información personal. Hoy, no están libres de ataques, alteraciones y robos informativos; que terminan afectando a la organización económicamente y en su imagen corporativa.

De esta manera, los riesgos informáticos como los códigos maliciosos y los hackers han ido evolucionando con el uso de la Internet. Estos riesgos se han incrementado debido a la integración de herramientas como elementos de hackeo de red, denegación de servicios y accesos no autorizados. A partir de esto se puede explotar las debilidades del sistema, dañar aplicaciones y corromper la información de la empresa; para estos casos se utilizará el escaneo de puertos.

El escaneo de puertos es una técnica que se usa con propósitos administrativos para auditar redes, con el fin de encontrar sus vulnerabilidades.

El resultado de ejecutar esta técnica revela los puertos que se encuentran abiertos y cerrados. Esto permitirá verificar el correcto funcionamiento de la infraestructura de seguridad (Software, antivirus, herramientas de respaldo, de monitoreo de la infraestructura de red y enlaces de telecomunicaciones, firewalls, soluciones de autentificación y servicios de seguridad en línea); de lo contrario, al estar en manos equivocadas podría ser usado con fines inadecuados en la red.

1.3- Problema de Investigación

1.3.1- Interrogación

¿Qué nos permite hacer la virtualización en lo que a seguridad se refiere?

1.3.2- Aseveración

La virtualización permite disminuir costos en inversión de Hardware de Networking, realizar pruebas de evaluación de herramientas de seguridad o ataques, gestionar y centralizar recursos de TI, lo que representa un gran ahorro y una ventaja de seguridad.[1]

1.3.3- Preguntas de investigación

- ¿Cuál es la frecuencia de los ataques por escaneo de puertos?
- ¿Cuál es la gravedad de estos ataques?
- ¿Qué herramientas existen para perpetuar estos ataques?
- ¿Qué herramientas existen para mitigar estos ataques?
- ¿Cuáles serían los usos que se podrían dar a estas investigaciones?

[1] Entrevista a Juan Carlos Yelmo García, orador principal de la 12ª. Conferencia Internacional sobre las TIC en la Seguridad Social. Disponible en el sitio Web de la Asociación Internacional de la Seguridad Social. Véase http://www.issa.int/esl/News-Events/News2/ICT-as-a-strategic-management-tool-A-basis-for-dynamic-social-security

1.3.4- Planteamiento de problema

El auge de la tecnología brinda nuevas posibilidades de mercados, desde simples registros de transacciones hasta todo tipo de comercio electrónico.

Todos estos avances positivos han hecho proliferar a la par nuevas formas de engaño, suplantación de identidad, robo de información y todo tipo de delitos informáticos que han permitido la aparición de hackers, los cuales pueden descubrir las vulnerabilidades de los sistemas con el fin de encontrar solución los problemas de seguridad o para descifrar información y vulnerar el sistema.

Los sistemas, desde su concepción, traen grandes fallas de seguridad que dejan la información de las organizaciones desprotegida ante intrusos internos o externos que buscan apropiarse de ella.

Frente a este problema, la investigación pretende averiguar soluciones de bajo costo para disminuir ataques por escaneo de puertos. Se utilizará plataformas experimentales como entornos virtualizados para disminuir, detectar la seguridad en redes por escaneo de puertos.

1.4- Justificación

El objetivo de este estudio es dar un enfoque práctico y descriptivo del ataque por escaneo de puertos, el cual es utilizado por administradores y usuarios no autorizados. Además, dar con posibles puertas de ingreso a la infraestructura de red mediante el uso de herramientas que permiten realizar el escaneo de puertos.

Este trabajo investigativo demostrará las posibilidades de uso de la técnica mencionada, es decir, el escaneo de puertos puede utilizarse tanto para fines lícitos o ilícitos. Por esta razón, la importancia de la investigación que planea enfatizar esta

dualidad informática para proponer mejores prácticas para que puedan ser implementadas.

La trascendencia del trabajo radica en brindar soluciones, basadas en los resultados del experimento que previene, detecta y reduce los riesgos de ataques por escaneo de puertos.

1.5.- Objetivos

1.5.1- Objetivo general

Diseñar e implementar una plataforma experimental basada en tecnología de virtualización que permita evaluar, controlar y mitigar los ataques reales por escaneo de puertos.

1.5.2- Objetivos específicos

- Analizar el estado del arte de soluciones al problema de escaneo de puertos basado en tecnologías de virtualización.
- Evaluar diversas herramientas que permitan atacar o defender el ataque de escaneo de puertos según sea necesario.
- Diseñar e implementar una plataforma experimental para la ejecución y evaluación del ataque por escaneo de puertos.
- Implementar la solución para detectar, controlar y mitigar los ataques por escaneo de puertos.
- Calcular los resultados y procesar estadísticamente las mediciones y evaluar resultados.

1.5- Alcance

Este estudio cubre algunas posibilidades de la técnica de escaneo de puertos para ser implementadas en una arquitectura de plataformas virtualizadas y estas mismas técnicas pueden ser probadas, documentadas y solucionadas de forma concreta. Este procedimiento estará registrado en la investigación propuesta en la Dirección de Posgrados de la Escuela Politécnica del Ejército (ESPE) que auspicia la investigación.

CAPÍTULO 2: MARCO TEÓRICO

2.1- Conceptos sobre conexiones TCP

TCP es un protocolo que significa Protocolo de Control de Transmisión (Transfer Control Protocol, en inglés), fue ejecutado como un proyecto de investigación, el cual pretendía agregar las redes desarrolladas por diferentes vendedores a la red de redes (Internet) (Forouzan, 2003). Algo que fue novedoso para su creación fue que proporcionaba algunos servicios básicos y que todos necesitaban como transmisión de archivos, correo electrónico e inicio remoto.

TCP es orientado a la conexión y además es considerado un protocolo de capa 4 (Transporte) en el modelo OSI, su envío se hace a través de flujo de datos y garantiza que la información llegue a su destinatario sin errores y en el mismo orden en el que fue enviado.

2.2- Estableciendo conexiones: sockets, puertos e IP's

Las conexiones TCP se realizan mediante dos tipos de negociación, cuando trata de conexión se usa la negociación 3-Way-Handshaking y cuando es desconexión es la negociación 4-Way-Handshaking.

Cuando se hace la negociación a tres pasos, lo primero que realiza el protocolo es abrir un socket en un puerto de tipo TCP y espera pasivamente en busca de nueva conexión, esto determina la parte servidor de una conexión TCP(véase Fig 2.1).

Por un lado, el cliente de la conexión TCP, efectúa una apertura activa de un puerto y envía un paquete SYN para iniciar la negociación a tres pasos, si la conexión es rechazada el servidor devuelve un paquete con el bit RST activado indicando que no

se puede establecer la conexión, pero si la conexión es realizada, la parte servidor de la conexión envía un paquete SYN/ACK validando así el enlace.

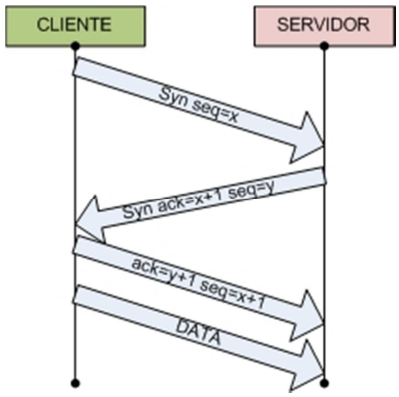

Fig 2.1: Establecimiento de conexión.

2.3- Desconexión TCP

El cliente debe emitir un paquete TCP con el bit activado en la bandera **FIN**, el cual indica el deseo de la finalización de una conexión(véase Fig 2.2) el servidor al revivir este paquete responderá con un nuevo paquete TCP con el bit de bandera anteriormente (**FIN**),posteriormente el servidor responde con un paquete TCP con el bit activado en bandera **FIN**, a su vez el servidor espera a que el cliente le responda con un paquete TCP con el bit activado en bandera **ACK**, desde este momento la conexión ha finalizado.

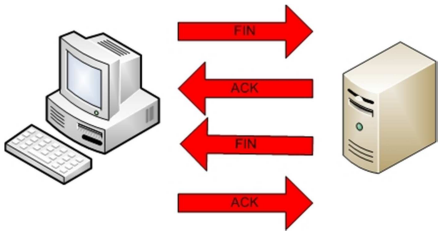

Fig 2.2: Finalización de conexión TCP.

En casos de que se estén transmitiendo datos, y se emita una paquete **FIN**, el receptor emitirá una respuesta **ACK**, esperará la finalización de transacción de datos y posteriormente se emitirá un paquete **FIN** por el receptor y un **ACK** por el emisor.

2.4- Conceptos de virtualización

2.4.1- Generalidades

La virtualización es una tecnología que apareció en los años 60, por la necesidad de aprovechar los recursos informáticos, dicha técnica permite particionar de una forma lógica un dispositivo físico con la particularidad de que el trabajo lo realizan en forma independiente usando recursos del mainframe (Fernández, 2008).

Con la aparición de las nuevas computadoras y la tecnología basada en el cliente servidor, las mainframes y sus aplicaciones virtualizadas fueron quedando rezagados para dar paso a la microcomputación, es decir, equipos potentes con tamaños reducidos de arquitecturas x86.

Considerando los recursos con los cuales se cuenta, se busca la optimización de los mismos, en el caso de servidores se trata de evitar el desperdicio de espacio, es por ello que se procede con la división del Hardware, con el fin de que las múltiples aplicaciones no produzcan conflictos entre sí, además se busca evitar el desperdicio de electricidad y dinero.

De esta forma los servidores aceptarán diferentes configuraciones, tales como diversos tipos de sistemas operativos, ya sea propietarios o de distribución gratuita, los cuales se los puede administrar de diferentes maneras considerando niveles de seguridad, y todo esto se lo hará de forma simultánea. De estas prácticas nace el concepto de virtualización, el cual ayuda a aprovechar al máximo los recursos físicos,

al configurar en un solo equipo varios entornos o máquinas con diferentes sistemas operativos, lo que conocemos como máquinas virtuales.

Entre los múltiples beneficios de dichas máquinas virtuales tenemos que se pueden configurar de tal forma que actúan como equipos independientes, a los cuales se les debe dar instrucciones de apagado y encendido. Además, tiene conexión a red, control de seguridad, acceso remoto, y se le puede asignar la cantidad de recursos deseados dependiendo de la necesidad que se tenga.

2.4.2- Virtualización de servidores

Virtualizar un servidor significa particionar el servidor físico en servidores virtuales(véase Fig 2.3) en donde se puede alojar distintos tipo de sistemas operativos, cada uno con sus recursos propios, independientes entre sí.(Gálvez Mozo, 2006)

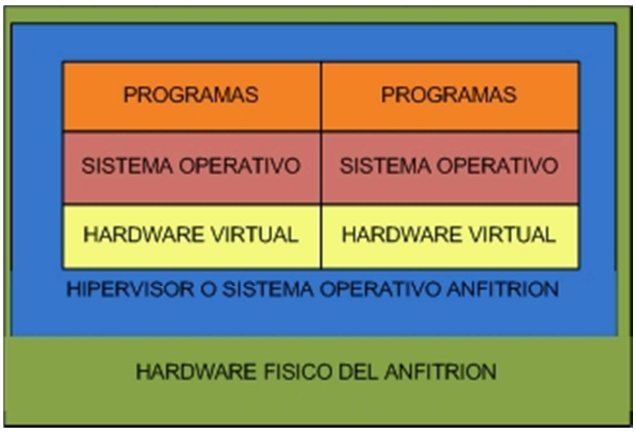

Fig 2.3: Virtualización servidores.

2.4.3- Virtualización a nivel de Hardware

Es la emulación del Hardware mediante máquinas virtuales, es decir, que el sistema operativo se ejecuta sobre Hardware virtualizado ya que se genera la capa

de emulación de recursos del computador. Se puede llevar a efecto la instalación de diferentes sistemas operativos (véase Fig 2.4).

Este tipo de virtualización nos permite correr Windows sobre Linux o viceversa, se puede tener más de una máquina virtual corriendo a la vez sin que el funcionamiento de una afecte a la otra, se debe tener en cuenta que por la cantidad de instrucciones que se ejecutan se experimenta un poco de lentitud en las mismas.

Fig 2.4: Virtualización Hardware.

2.4.4- Virtualización a nivel del sistema operativo

La virtualización mediante Software no realiza emulación del Hardware, los procesos que se ejecutan son aislados y trabajan con cada servidor virtual, esta virtualización se realiza sobre un Sistema Operativo con un Software hypervisor que es un programa para llevar adelante la virtualización, el cual nos permite instalar distintos sistemas operativos(véase Fig 2.5),que trabajan de forma independiente ya que el servidor físico es dividido en múltiples particones que emulan a un servidor real.(Quétier, Neri, & Cappello, 2006)

Entre los hypervisores para realizar este tipo de virtualización tenemos:

- VMware

- VirtualBox
- Hyper-V
- OpenVZ
- FreeBSD Jails
- Citrix XenServer

A este tipo de virtualización la conocemos como virtualización por contenedores, los cuales trabajan de forma independiente, es decir, que si una de las máquina deja de funcionar no afecta a la otra, y así se gana en rendimiento de los equipos virtuales.

Ejecuta servidores privados virtuales con su kernel, que está encargado de asignar los recursos para cada servidor, los cuales tendrán su espacio propio en disco, memoria ram, red y se podra reiniciar independientemente de los otros servidores, es necesario mencionar que si el kernel tiene problemas todos los SO no funcionaran bien.

Este tipo de virtualización es recomendado por el uso eficiente que se le da a los recursos físicos del anfitrión gestionando los recursos del kernel para cada sistema operativo que lo necesite, se debe mencionar también que entres sus desventajas limita la elección del sistema operativo ya que se debe a la compatibilidad entre anfitrión y SO.

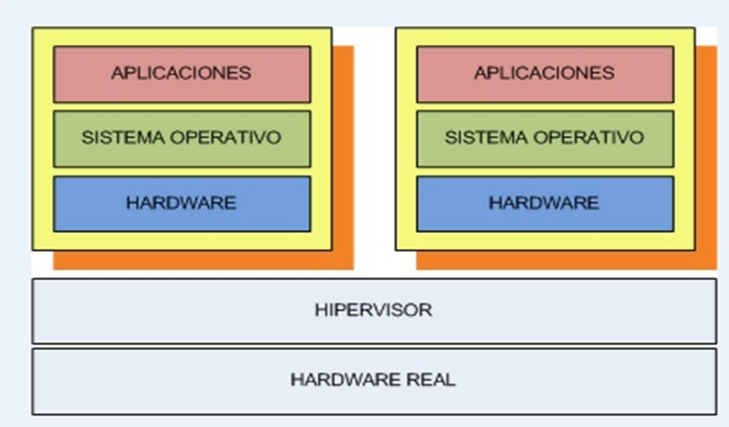

Fig 2.5: Virtualización por Software.

2.4.5- Aplicaciones

En el mercado existen múltiples tipos de aplicaciones, las cuales sirven para realizar la virtualización de origen libre, gratuito o pagado, la aplicación a escoger dependerá:

- ✓ De las características del Hardware
- ✓ Del tipo de sistema operativo
- ✓ De las razones para virtualizar
- ✓ Del fin comercial o personal

2.4.6- Sistema operativo

El sistema operativo que se use depende mucho la elección de la aplicación, para virtualizar existen versiones multiplataforma, como VMware que puede ser de versiones gratuitas o pagadas, Virtual Box que funciona sobre Windows, Linux, Mac. Entre estas aplicaciones que se tiene en el mercado se puede escoger por la licencia gratuita, pagada, Software libre entre otras, cabe mencionar que en el caso de Mac se puede usar el VMware Fusion 3.

2.4.7- Aplicaciones para virtualización

De acuerdo con las necesidades para las cuales se considere virtualizar se debe escoger la aplicación, por ejemplo, si se necesita trabajar con gráficos de alta resolución o si se va a usar gráficas 3d, se puede utilizar Hyper-V.

Si lo que se busca es rendimiento para las aplicaciones que se va a soportar en las máquinas virtuales se recomienda Hyper-V, Virtual Box, VMware, si se desea ambientes sencillos de operar, la mejor opción sería Virtual Box, aunque en la actualidad las aplicaciones para virtualizar cada vez presentan interfaces más amigables con el usuario (véase Fig 2.6).

Fig 2.6: Aplicaciones para virtualizar.

2.5- Técnicas de escaneo

2.5.1- ACK Scan

ACK Scan a diferencia de las demás técnicas, nos permite detectar con exactitud el puerto que se encuentre en modo silencio, empleando este procedimiento como apoyo secundario la utilización de la misma después de un método ya mencionado, resulta ser muy poderoso para determinar si el puerto se encuentra abierto o en

silencio. A la vez puede ser como apoyo para escanear computadoras que se encuentren tras un Firewall, ya que este no acepta intentos de conexión (**SYN**). Su funcionamiento se basa en el envío de paquetes ACK con números de secuencia confirmación de forma aleatoria, cuando el puerto reciba este paquete y esté abierto o cerrado responderá con un paquete **RST**, pero si no se obtiene respuesta entonces el puerto está en modo silencio(Cantú,2011)(véase Fig 2.7).

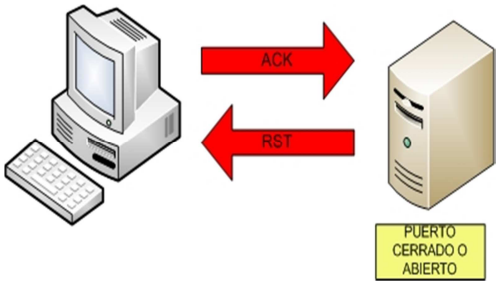

Fig 2.7: ACK Scan.

2.5.2- NULL Scan

Este escaneo es similar al **TCP FIN**, con la particularidad de que el cliente debe emitir un paquete TCP con todas las banderas desactivadas, así se debe observar lo siguiente del lado del servidor:

- Si el servidor responde con un **RST**, entonces el puerto está cerrado.
- Si no responde, el puerto está abierto o en silencio.

La única ventaja que tiene este escaneo, es que ciertos Firewalls vigilan los intentos desconexión (**SYN**) y finalización de conexión (**FIN**), de modo que resulta necesario este escaneo cuando se presente un problema de este tipo(Cantú,2011) (véase Fig 2.8).

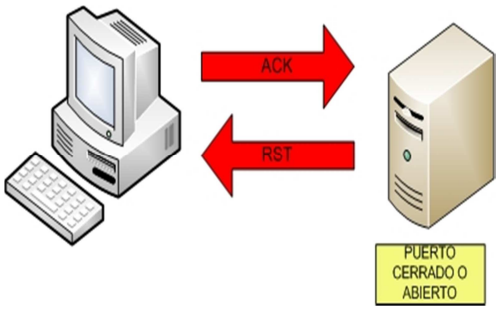

Fig 2.8: Null Scan.

2.5.4- Xmas Scan

En este escaneo se debe activar las banderas **FIN/URG/PSH** y esperar como respuesta:

- Si el servidor responde con un **RST**, el puerto está cerrado.
- Si no responde, entonces está abierto o en silencio.

Las desventajas son que el escaneo solo se hace a computadoras que no estén tras un Firewall que vigile paquetes **SYN** y **FIN** (Cantú,2011).

2.5.5- SYN/ACK Scan

El escaneo SYN/ACK es muy potente frente a equipos que están tras un Firewall o IDS sencillo, ya que este paquete solo engaña al servidor avisándole que hubo un error en la transacción (nunca estuvo conectado). Asimismo surgen estos efectos:

- Si el servidor responde con un **RST**, el puerto está cerrado.
- Si no responde, el puerto está abierto o en silencio (Cantú,2011).

2.5.6- RPC Scan

El escaneo RPC tiene por objetivo encontrar aplicaciones RPC (Remote Procedure Calls) a partir de puertos encontrados por una técnica de escaneo TCP o UDP, por ejemplo: SYN Scan. Una vez que haya encontrado la aplicación este

protocolo es capaz de ejecutar código remotamente, por lo cual implica un riesgo a gran escala si esta técnica logra su objetivo (Cantú,2011).

2.5.7- Zombie Scan

Este sistema se realiza para no ser detectado por el servidor que se desea escanear, es decir, que la IP no llegue a ser detectada por el servidor, y a cambio de esto se registre un IP que no es la del host original. Es necesario contar con un Host Zombi, es decir, una computadora conectada a Internet y que su tráfico sea muy bajo o en su defecto nulo.

Primero se realiza al Host Zombi un **ping** que nos permita ver el campo **ID** de la cabecera **IP** y el resultado sería:

50 bytes from 10.10.10.10: seq=1 ttl=64 id=+1 win=0 time=96 ms
50 bytes from 10.10.10.10: seq=2 ttl=64 id=+1 win=0 time=88 ms
50 bytes from 10.10.10.10: seq=3 ttl=64 id=+1 win=0 time=92 ms

Como se ilustra arriba, el campo **ID** está en 1, se puede decir que el tráfico es nulo.

El siguiente paso es realizar un paquete con el IP falseado (spoofing) que contendrá la IP Origen del Host Zombi, de este modo el intento de conexión se efectuará hacia el servidor con una IP origen del Host Zombi, de modo que surgirán los siguientes efectos:

- Si el servidor envía un SYN/ACK, indica que el puerto está abierto en Servidor, y al recibir este paquete el Host Zombi retornará un paquete RST, es aquí donde se genera un pequeño tráfico de datos.
- Si el servidor envía un RST/ACK, indica que el puerto está cerrado y al recibir este paquete el Host Zombi, no realiza ninguna contestación, es decir que el tráfico sigue nulo.

- Si el servidor no pone en ejecución contestación, entonces el puerto estará en silencio, y el Host Zombi estará aún con tráfico nulo.

Este modo de operar es un estándar establecido dentro de la implementación de la pila TCP/IP.

A continuación se observa de nuevo el estado del ID, en el ping constante después de enviar el paquete falseado.

50 bytes from 10.10.10.10: seq=10 ttl=64 id=+1 win=0 timw=96 ms
50 bytes from 10.10.10.10: seq=11 ttl=64 id=+2 win=0 timw=80 ms
50 bytes from 10.10.10.10: seq=12 ttl=64 id=+3 win=0 timw=92 ms
50 bytes from 10.10.10.10: seq=13 ttl=64 id=+2 win=0 timw=96 ms
50 bytes from 10.10.10.10: seq=14 ttl=64 id=+1 win=0 timw=80 ms
50 bytes from 10.10.10.10: seq=15 ttl=64 id=+1 win=0 timw=92 ms

Como se detalla, el puerto del servidor está abierto, ya que el Host Zombi (10.10.10.10) tuvo un incremento en el campo **ID**, esto indica que hubo una interacción entre el servidor y el Host Zombi. En caso que estuviese cerrado o en silencio el puerto del servidor, el estado ID de Host Zombi (10.10.10.10) sería uno (Cantú,2011).

2.6- Herramientas de seguridad y análisis de vulnerabilidades

2.6.1- NMAP (Mapeador de redes)

NMAP es una herramienta usada para ejecutar la auditoría de las seguridades de las redes, con la cual se realiza análisis de cada paquete IP, por lo general los administradores de las redes llevan adelante inventarios de las mismas ya que NMAP trabaja con información DNS, en la cual se considera el tipo de puerto, protocolos, estados de los puertos y las direcciones Mac que están vinculados a dichos puertos.

Un puerto puede tener tres tipos de estado: estado abierto o estado de escucha, cerrado o estado de no escucha y en estado de filtrado donde el estado del puerto es indeterminado. (NMAP)

2.6.2- Características NMAP

NMAP tiene las siguientes características:

- Identifica Host dentro de una red con el uso del ping.
- Lista los puertos por estado y tipo de protocolo.
- Determina el tipo de sistema operativo.
- Determina la aplicación que corre sobre cada puerto.
- Lista características de Hardware del computador.
- Es una de las herramientas más usadas por los hackers.
- Usado para no ser detectado por IDS.
- Es compatible con sistemas operativos como: Windows, Linux, Solaris, Mac OS, BSD.
- Trabajo bajo línea de comandos y también de forma gráfica como: Zen NMAP.
- Es usada como herramienta de administración para encontrar fallas de seguridad en la red y como herramienta de ataque para encontrar vulnerabilidades en las redes como medio de ataque.
- Es una herramienta de código abierto.
- Sirve para determinar el tipo de Firewalls que se usan.
- Trabaja bajo licencia GNU GPL.

2.6.3- Wireshark

Wireshark es una herramienta que actúa directamente sobre la red, analizando el tráfico, es un instrumento de código abierto, que implementa filtros para realizar las búsquedas; soportan aproximadamente 1 100 puertos, posee además una interfaz fácil de usar, esta herramienta corre sobre sistemas operativos como Windows, Linux, Mac Os, presenta una aplicación portable.(Orebaugh, 2007)

Wireshark trabaja en dos versiones por línea de comandos llamada t-sharky gráfica, cabe mencionar que esta herramienta nos permite analizar los protocolos, fue conocido como Ethereal, usado para solucionar problemas en las redes, también es una herramienta didáctica de enseñanza de redes. Wireshark incluye un completo lenguaje para filtrar y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

- Trabaja en modo promiscuo.
- Software Libre.
- Utiliza permisos de Administrador.
- Utiliza licencia GPL.
- Captura datos en tiempo real directo desde la red o lee datos desde un archivo previo.
- Utiliza librería PCAP.
- Emplea archivos TCPDUMP.
- Trabajo con la mayoría de protocolos.
- Es utilizado en múltiples plataformas.
- Corre sobre Linux, Windows, Solaris, Mac OS X.

- Presenta información detallada del análisis de la red.
- Mantiene logs de los paquetes capturados.
- Realiza filtrado por paquetes de la información analizada.
- Búsquedas ordenadas por protocolos.
- Permite obtener estadísticas de los resultados.

2.7- Metodologías o estándares de seguridad aceptados

2.7.1- 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(ISO.ORG)

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.

2.7.2- OSSTMM

Open Source Security Testing Methodology Manual, es una norma desarrollada para test de Intrusión y verificación de hechos. Su objetivo en mira es medir cómo 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 hacen 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 está 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.[2]

[2] (Open Source Security Testing Methodology Manual (OSSTMM), 2010).

CAPÍTULO 3: DISEÑO Y CONSTRUCCIÓN DE LABORATORIO DE PRUEBAS

3.1- Introducción

Este capítulo describe en detalle el laboratorio que se ha creado para este trabajo, con el uso de diagramas, se muestra el diseño de los diferentes segmentos de red, con sus respectivos servicios, equipos virtualizados y sus configuraciones.

Además, se detalla la configuración inicial del cortafuegos (TMG) y como fue definido para que provea los diferentes servicios en la red, ya que dicha configuración es el primer escalón en este trabajo.

3.2- Diseño de la arquitectura

En la Figura 3.1 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 redes creadas que son la red interna, DMZ y red externa, 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 red.

También, se ha designado de 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.
    - 3 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.
    - 4 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.

3.2.1- Diagrama Físico

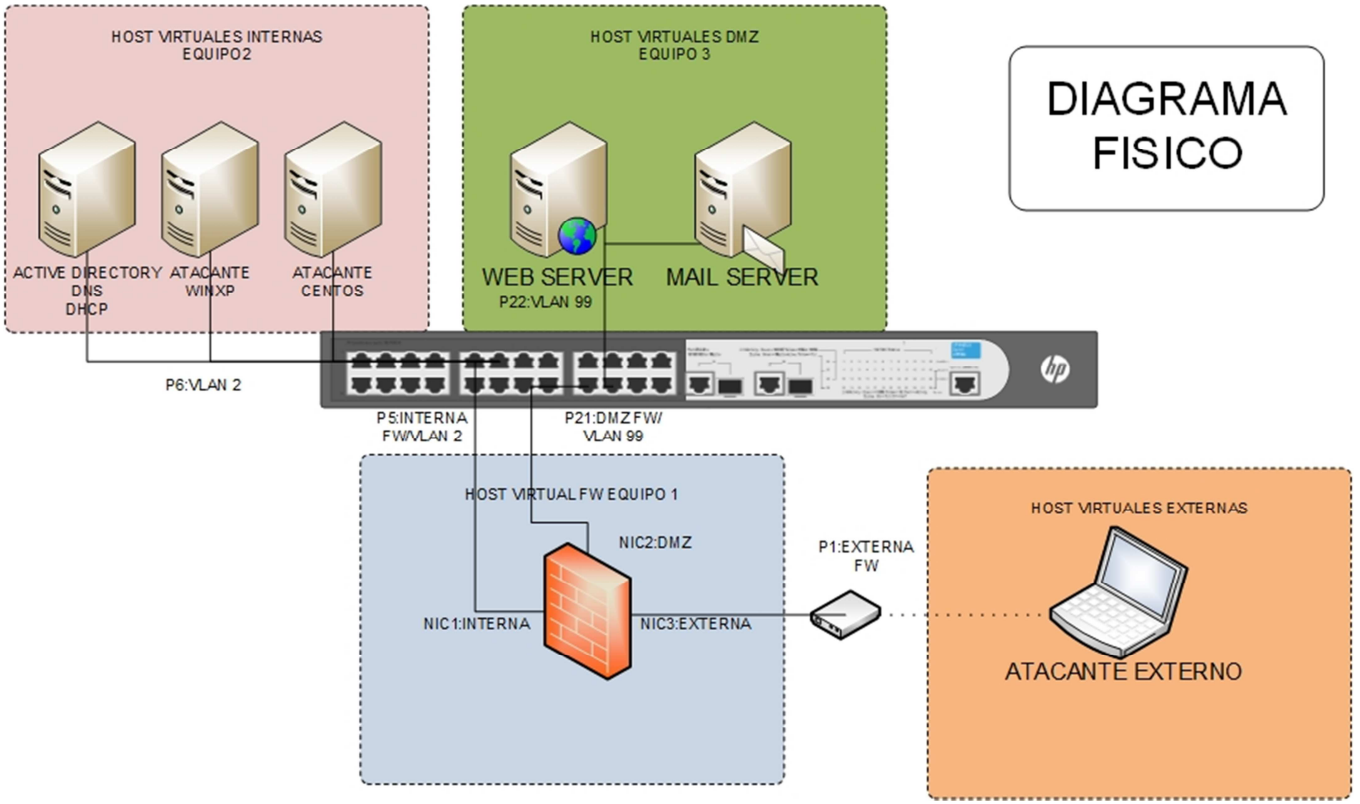

Fig 3.1: Diagrama Físico.

En la Figura 3.2, se encuentra el diagrama lógico que describe los segmentos de red empezando por la red interna con el rango de direcciones IP (192.168.0.0) y contiene una serie de servidores y estaciones dedicadas para el ataque de la red interna del laboratorio de manera estratégica. Es importante resaltar que en esta parte de la red, se encuentran servicios sensibles, como directorio activo, DNS y DHCP, que proveen resolución de nombres, manejo de usuarios, accesos, permisos y enrutamiento, respectivamente son servicios ampliamente usados en el ámbito empresarial y dan una visión más real a este laboratorio.

En el segmento de red externa, con rango de IP (192.168.1.0) de igual manera que el segmento interno, este contiene un servicio para esta investigación, como es el de VPN, el cual provee la conectividad al laboratorio a través de Internet, y es usado para poder dar acceso a las estaciones virtuales designadas para atacar externamente esta infraestructura. Para lograr este objetivo se utilizó una IP Pública provista por el proveedor de Servicio de Internet, y el protocolo PPPoE que se usa para encapsular las tramas en Ethernet y es necesario para implementar el servicio de VPN.

Finalmente, se encuentra la red de la DMZ, con rango de IP (192.168.2.0), donde se pueden observar los servicios de Web (HTTP) y correo electrónico (SMTP), los mismos que son típicamente designados a esta red, porque deben salir hacia Internet ya que el concepto de DMZ, es el de proveer una capa más de seguridad para los servicios que deben ser consumidos externamente, con el objetivo de separar nuestra red interna, de cualquier atacante fuera de nuestra organización. Hay que recalcar que la diferencia de conectarse mediante el segmento externo y la DMZ radica en que el usuario que se conecta mediante el segmento externo, es un usuario registrado en

esta infraestructura (Extranet), y el usuario de la DMZ es un usuario no registrado, que consume los servicios provistos en la DMZ mediante Internet.

Para la implementación de este trabajo se ha tratado de virtualizar la mayoría de equipos, tanto de red como servidores y estaciones, tal es el caso que se cuenta con siete máquinas virtualizadas, de las cuales cuatro son servidores, dos atacantes interno - externo respectivamente y una sola hospeda el cortafuegos que cumple también la función de ruteo entre los diferentes segmentos de red.

Por lo cual, es importante entender que los diferentes segmentos de red contienen servicios y son provistos en la infraestructura mediante un equipo virtual que cumple la función de un Router, con esto, se garantiza un entorno completamente experimental y controlado.

3.2.2- Diseño Lógico

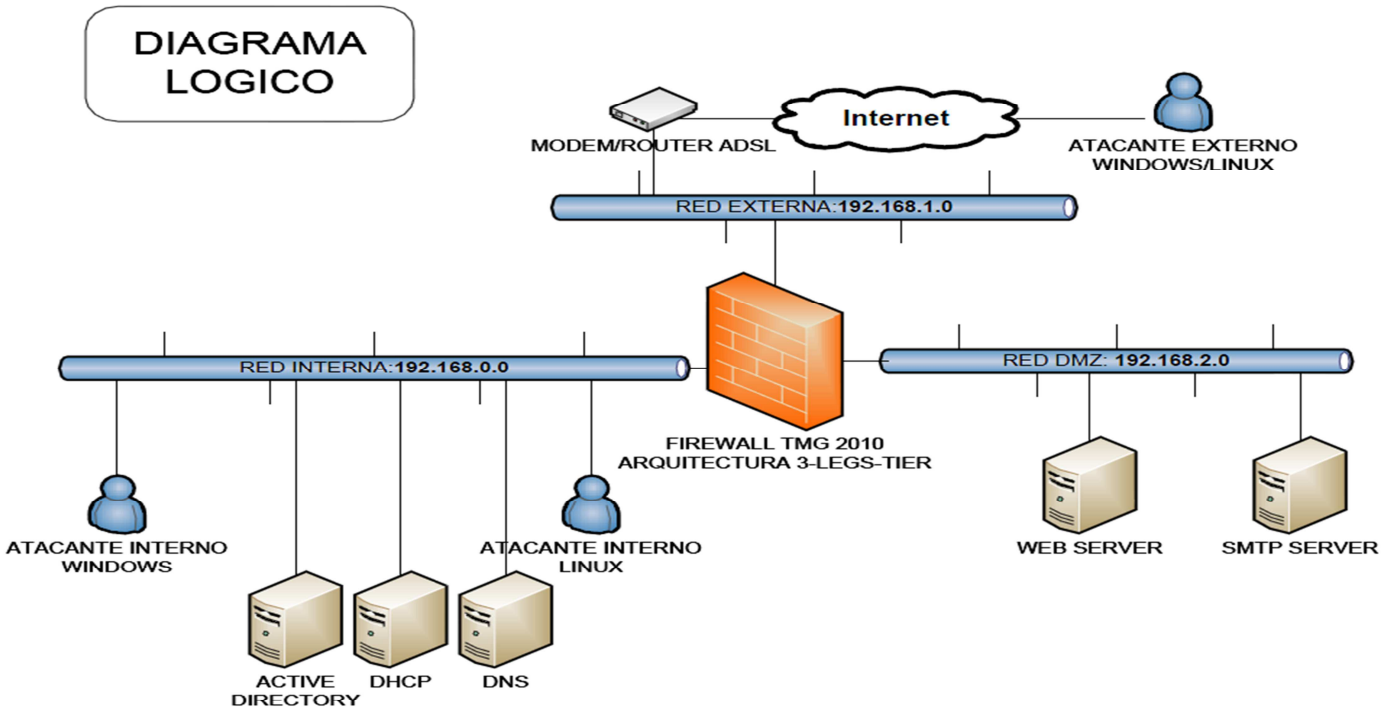

Fig 3.2: Diagrama Lógico.

En la Figura 3.3, se encuentra el diagrama de servicios, el cual muestra cada equipo con nombre, 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 definitiva, este diagrama es la configuración inicial de este laboratorio, la línea base de este trabajo y el producto final del diseño de esta infraestructura, que ha sido basada en estándares para su construcción.

3.2.3- Diseño de los servicios de la red

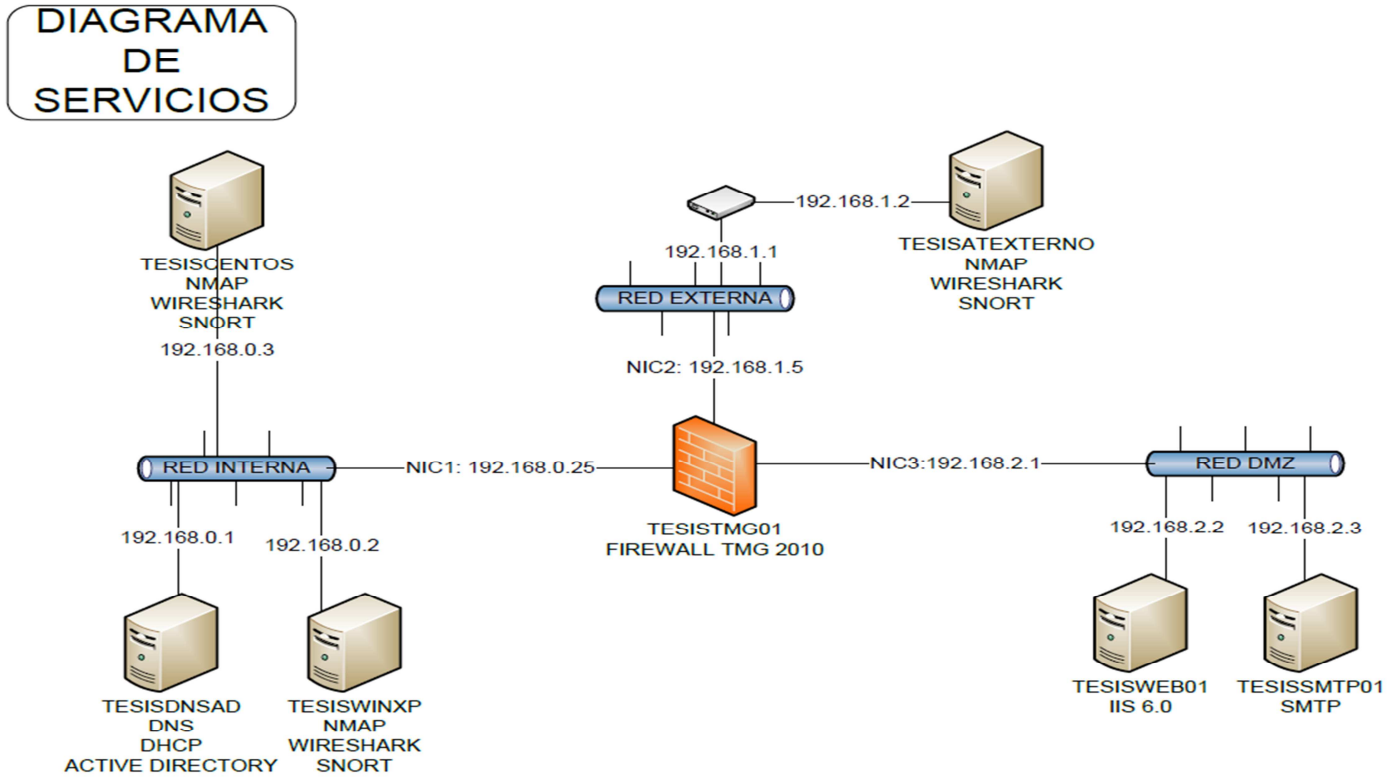

Fig 3.3: Diagrama de Servicios.

3.3- Configuración de la plataforma de experimentación, Línea Base

Las reglas de Firewall están divididas en dos partes: a nivel de red y de acceso a Internet. Al hablar de reglas de red se hace referencia a las que permiten accesibilidad entre sistemas de los segmentos de red, es importante notar que el concepto de Firewall determina que absolutamente todo elemento de red que se encuentre en la infraestructura está bloqueado por default, por lo cual se deben agregar estas reglas para habilitar los accesos a servicios dispuestos en la infraestructura.

En la Figura 3.4 se observa un conjunto de reglas agrupadas de la forma mencionada, en el cual se destacan dos comúnmente usadas, como es el acceso a DNS corporativos y el acceso a las privadas y públicas.

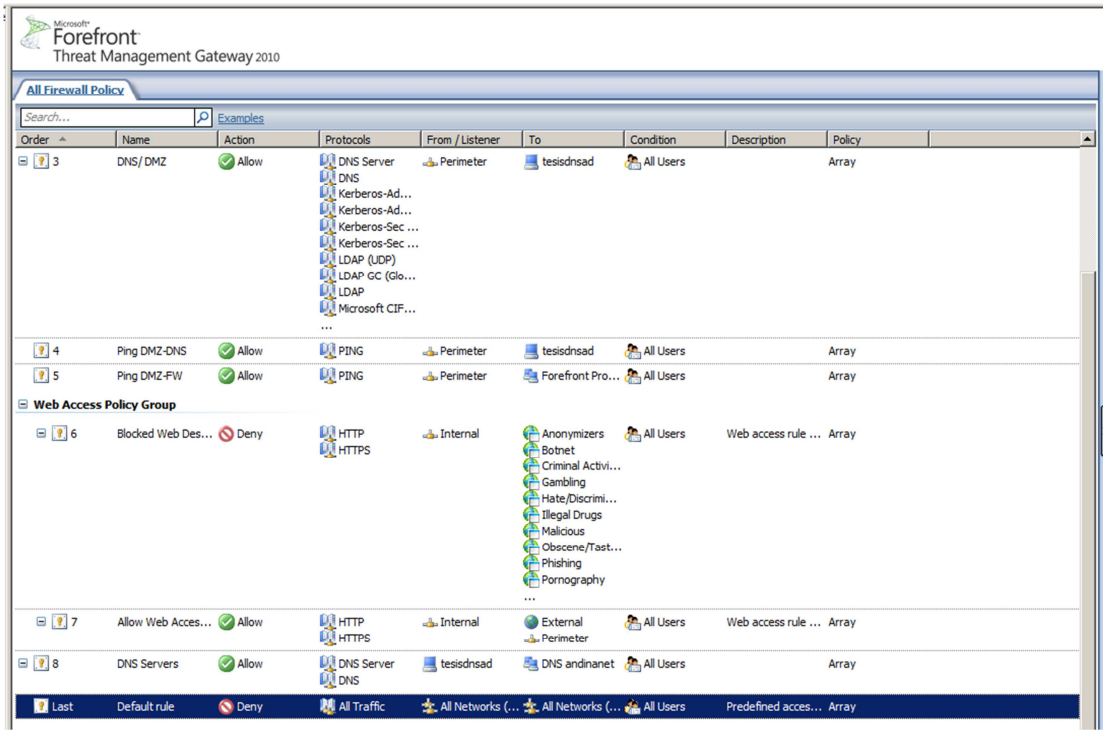

Fig 3.4: Reglas de Firewall.

La razón de la existencia de estas reglas es proveer servicios a los diferentes segmentos de red, como por ejemplo, el consumo del DNS a la DMZ o servicios de ping (ICMP) hacia los diferentes servidores para comprobar conectividad, en el caso de la regla del ping, se activa ocasionalmente solo para comprobación de conectividad ya que en una red corporativa no se debe proveer ping(ICMP) en servidores corporativos.En la sección de reglas para Internet, como se muestra en la Figura 13, proveen acceso Web a los distintos ordenadores dentro de la infraestructura, siendo importante recalcar que las reglas del Firewall creadas en esta sección funcionen para filtrar contenidos y proveer acceso de Internet al laboratorio virtualizado.

Existen dos reglas comunes en su uso de gran importancia en esta sección:

a. Como se ve en la Figura 3.5, Allow Web Access permite la conexión hacia cualquier servicio de tipo http y https, a través de la interface externa hacia la interna, en esta regla se podrían aumentar protocolos como FTP, SMTP, entre otros.

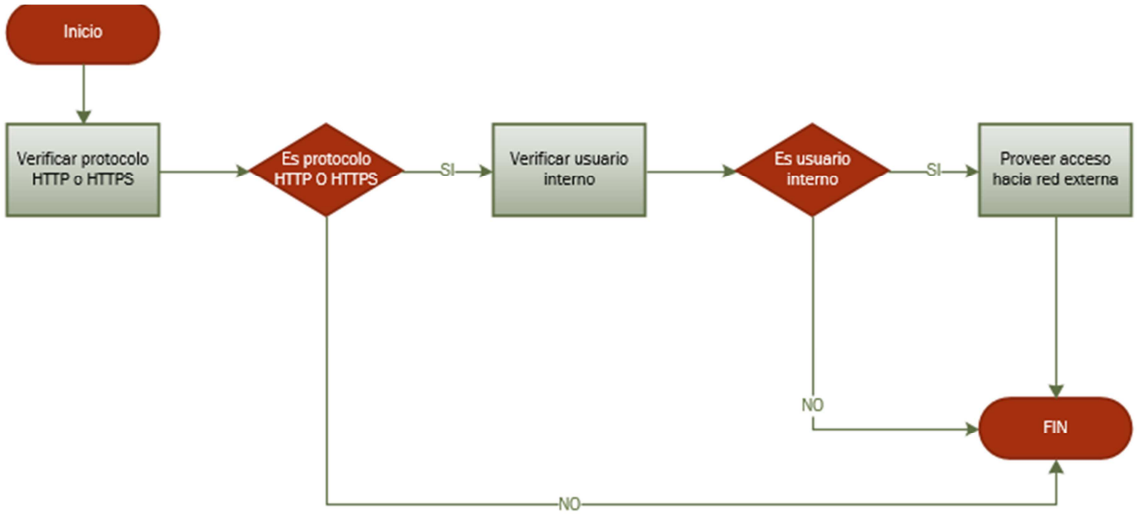

Fig 3.5: Regla Allow Web Access.

b. Como se ve en la Figura 3.6, existe la regla DNS Server que es prioritaria y se usa en arquitectura de tres patas ya que permite la conexión hacia los DNS servers del proveedor de internet, sin la existencia de esta regla no se podría proveer del servicio de Internet.

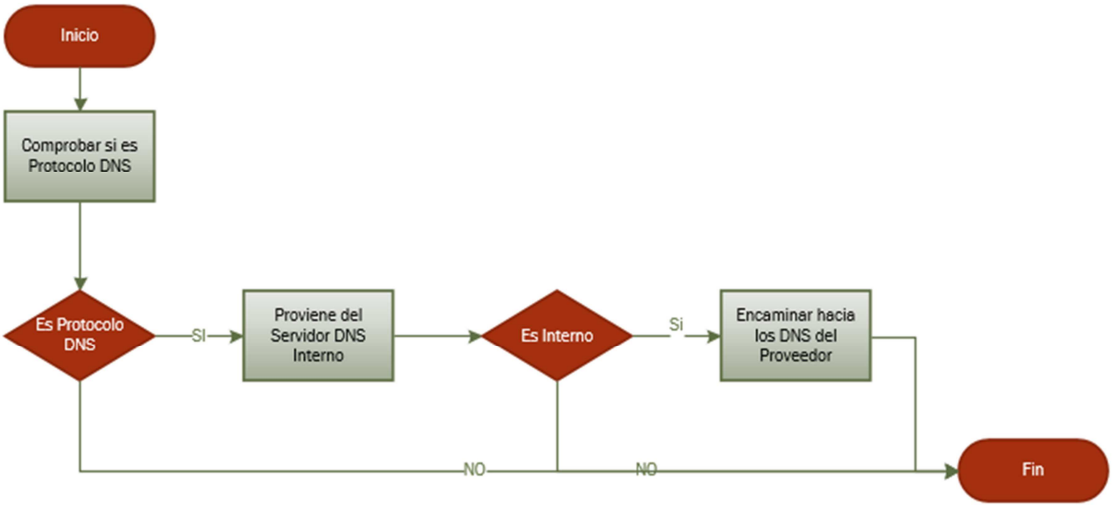

Fig 3.6: Regla DNS Server.

CAPÍTULO 4: PROPUESTA PARA DETECTAR, CONTROLAR Y MITIGAR ATAQUES POR ESCANEO DE PUERTOS

4.1- Introducción

En este capítulo se encontrarán las pruebas con sus respectivas muestras y análisis de los resultados. También se debe recalcar que para este trabajo se ha decidido tomar muestras de los siguientes ataques:

- TCP Connect() Scan
- UDP Scan
- ACK Scan
- NULL Scan

Dichas pruebas se realizaron usando un capturador de paquetes Wireshark y NMAP, que serán descritos a lo largo de este capítulo.

4.2- Toma de datos

En la toma de datos se han obtenido tres muestras por cada tipo de ataque, diferenciando el tipo de red, es decir, se han separado los datos obtenidos tanto para red Interna con DMZ y de la Red Externa (Open Source Security Testing Methodology Manual (OSSTMM, 2010).

Cada conjunto de datos realizado, fue tomado desde un computador virtualizado y localizado estratégicamente para efectuar los ataques en cada segmento de red.

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, que se muestran en la Tabla 4.1 son los siguientes:

Tabla 4.1: 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

Fuente Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

Una característica importante en este tipo de ataque es el poder descubrir topologías de red(véase Fig 4.1) y puertas abiertas que son los puertos, por lo cual el gráfico de topología de la red interna que fue obtenido por NMAP es un indicio de que el ataque fue satisfactorio.

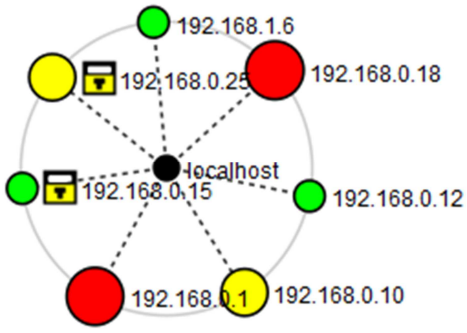

Fig 4.1: Topología de red.

Este gráfico 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.

Con respecto a las particularidades en cada uno de los ataques hemos encontrado los siguientes datos que han sido consolidados a través de las muestras tomadas y nos señalan puertos abiertos en cada ataque.

Para el ataque TCP se ha encontrado que en los tres ataques propuestos por este trabajo, se han repetido más de una vez los puertos presentados en la Tabla 4.2 que se muestra a continuación:

Tabla 4.2: Resultados de ataque escaneo TCP Connect().

TCP	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25	192.168.1.4
	53	135	22	80	80
	80	139		445	
	88	443		8080	
	135				
	139				
	389				
	445				
	1027				
	1097				

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

En esta tabla se puede observar puertos críticos como el puerto 22 que es SSH, lo cual denota que se trata de una arquitectura Linux, puertos de administración como el 389 de Active Directory, lo que para un atacante denota un servidor de suma importancia.

En el caso del escaneo UDP, se presentan los resultados en la Tabla 4.3, donde como primera conclusión se observa que se ha encontrado una lista más grande de puertos que se han repetido más de una vez en las tres muestras tomadas, y se

evidencia lo vulnerable que es la infraestructura presentada, sin las mejoras respectivas en el Firewall corporativo.

Tabla 4.3: Resultados de ataque escaneo UDP.

UDP	192.168.0.1	192.168.0.10	192.168.0.1	192.168.0.25	192.168.1.4
	53	123	158	ninguno	80
	123	137	17836		
	137	138	19039		
	1040	445	21298		
	67	5000	28641		
	68	1030	30704		
	88	1031	32776		
	138	1032	34861		
	389	1033			
	445	1036			
	464	1040			
	500	1041			
	1035	1043			
	1036	1900			
	1044	4500			
	1050				
	1054				
	1056				
	1060				
	1070				
	4500				

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

En la Tabla 4.4 se muestran los resultados del ataque NULL Scan, el cual evidencia, ser un ataque menos efectivo por la cantidad de puertos que enlista, pero sin embargo, de igual manera que el ataque TCP muestra algunos equipos críticos y puertos asignados a los protocolos dentro de la infraestructura propuesta.

Tabla 4.4: Resultados de ataque NULL Scan.

ACK	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25	192.168.1.4
	53	443	22	80	80
	80			445	
	88			8080	
	135				
	139				
	389				
	445				
	1027				
	1097				

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

Finalmente, para el ataque ACK, como se muestra en la Tabla 4.5, se observa que es un ataque menos efectivo ya que no muestra muchos puertos, pero sin embargo, evidencia puertos críticos en algunos equipos de la red.

Tabla 4.5. Resultados de ataque ACK Scan.

ACK	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25	192.168.1.4
	53	443	22	80	80
	80			445	
	135			8080	
	139				

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

En cuanto a red se han obtenido métricas de consumo de ancho de banda, y tiempos de retardo en cada host estos datos fueron tomados por la herramienta Wireshark.

En la tabla 4.6 se muestran los consolidados para el ataque TCP, en cuanto a paquetes, tiempos de retardo, tamaños y tiempos de transferencias, de las tres 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 4.6: 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

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

En la Tabla 4.7, se muestran los consolidados, para el ataque UDP, en cuanto a paquetes, tiempos de retardo, tamaños y tiempos de transferencias, de las tres muestras propuestas, mediante la herramienta Wireshark.

Tabla 4.7: 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

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

En la Tabla 4.8 se muestran los consolidados, para el ataque Null Scan, en cuanto a paquetes, tiempos de retardo, tamaños y tiempos de transferencias, de las tres muestras propuestas, de igual manera fueron tomados por Wireshark.

Tabla 4.8: 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

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

En la Tabla 4.9 se muestran los consolidados para el ataque ACK Scan, en cuanto a paquetes, tiempos de retardo, tamaños y tiempos de transferencias de las tres muestras propuestas, mediante la herramienta Wireshark.

Tabla 4.9: 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

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

4.3- Procesamiento estadístico de datos (Línea Base)

En las Figuras 4.2 y 4.3 se muestran con histogramas los tiempos de culminación por cada tipo de ataque en cada segmento de red, en el cual se puede ver que el ataque Null Scan es el que más tiempo toma, sin embargo como se describió anteriormente no es el ataque más efectivo:

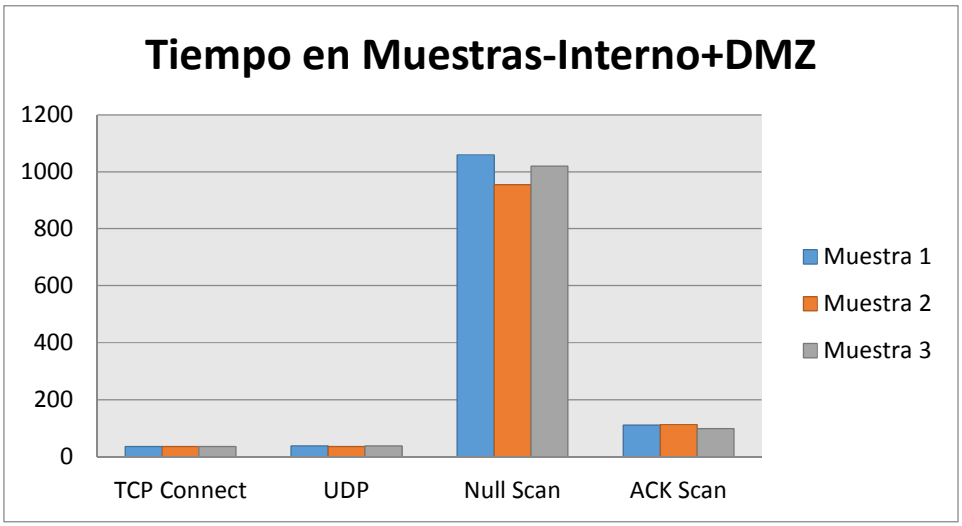

Fig 4.2: Datos estadísticos red interna.

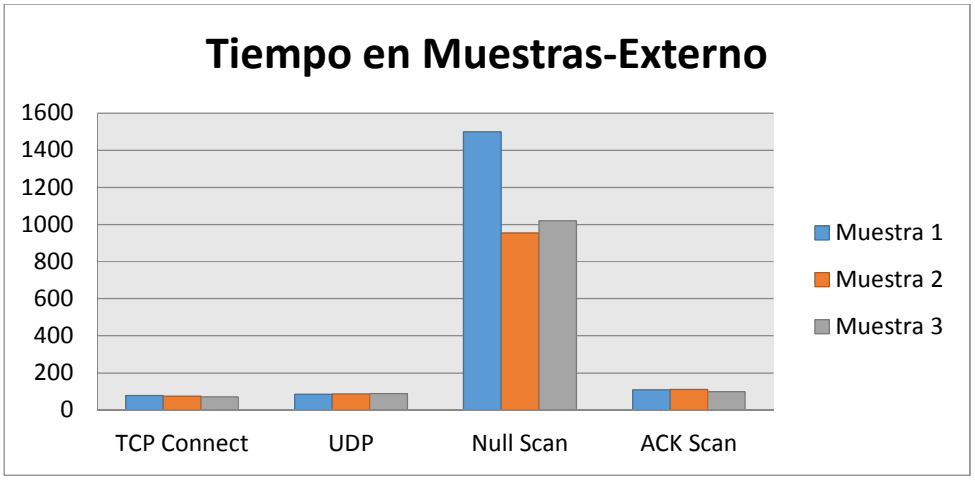

Fig 4.3: Datos estadísticos red externa.

En la Figura 4.4 se muestra el histograma de los paquetes enviados, como se observa en el gráfico, el ataque TCP es el ataque con mayor número de paquetes enviados.

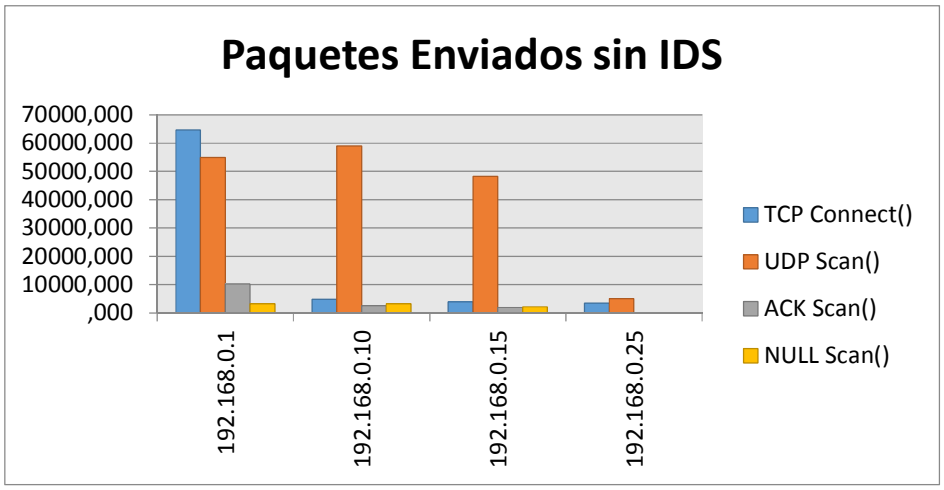

Fig 4.4: Datos estadísticos por paquetes.

Finalmente, la Figura 4.5 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.

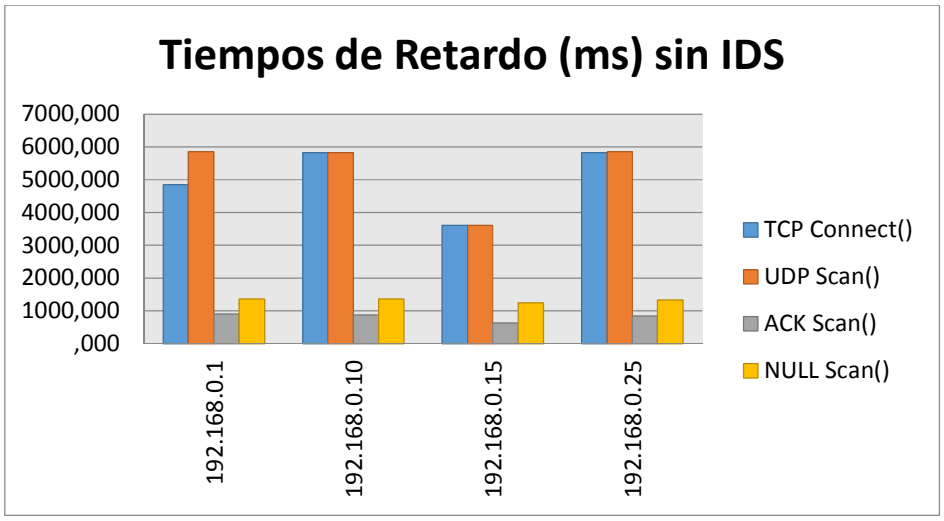

Fig 4.5: Tiempos de Retardo sin IDS en ms.

4.4- Algoritmo para detectar, controlar y mitigar ataques por escaneo de puertos.

Para bloquear este tipo de ataque se activó el IDS del Firewall, se experimentó en el laboratorio de pruebas y se han obtenido los siguientes resultados.

Para evitar el ataque TCP, se propuso la siguiente regla, en el Firewall, como se muestra en la Figura 4.6

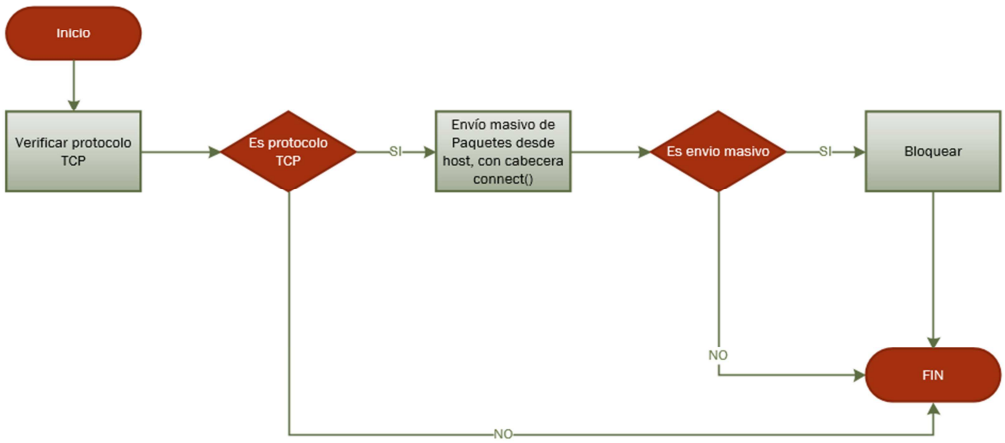

Fig 4.6: Regla Firewall TCP Scan.

Para el ataque de UDP Scan se ha propuesto la siguiente regla, como se ve en la Figura 4.7, ya que el patrón muestra un gran envío de paquetes UDP cada segundo:

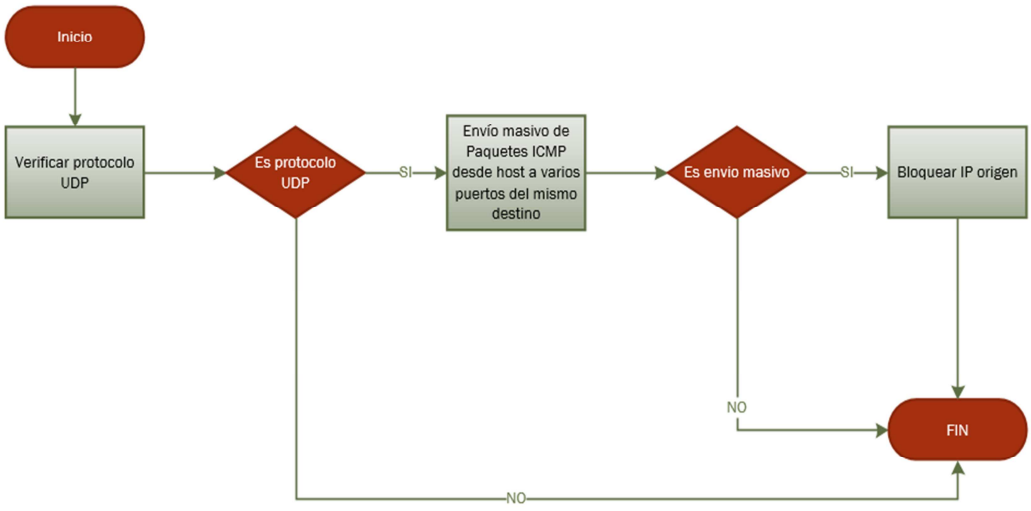

Fig 4.7: Regla Firewall UDP Scan.

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 4.8

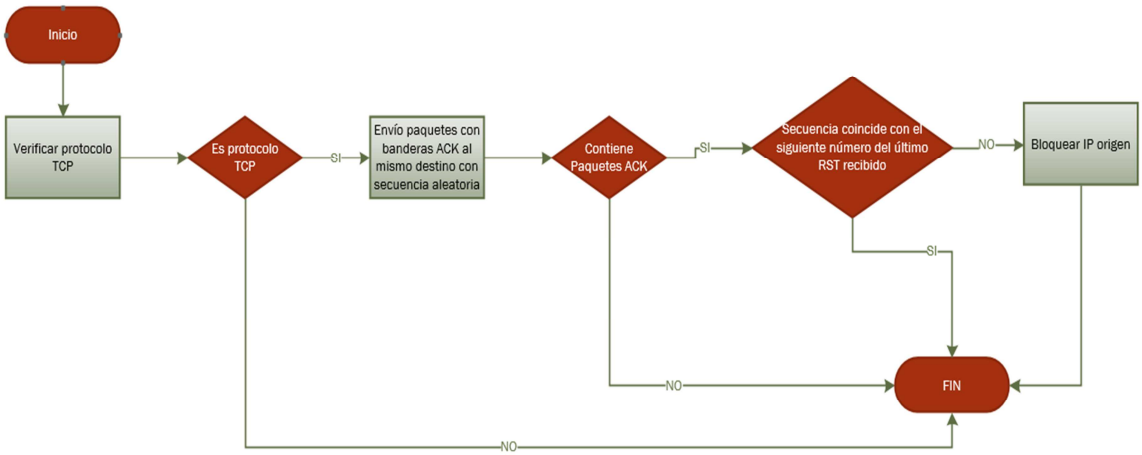

Fig 4.8: Regla Firewall ACK Scan.

Para el ataque NULL Scan, es más complejo ya que se tiene que revisar las llamadas de múltiples banderas desde el mismo origen y mandadas al mismo tiempo, como se puede ver en la Figura 4.9

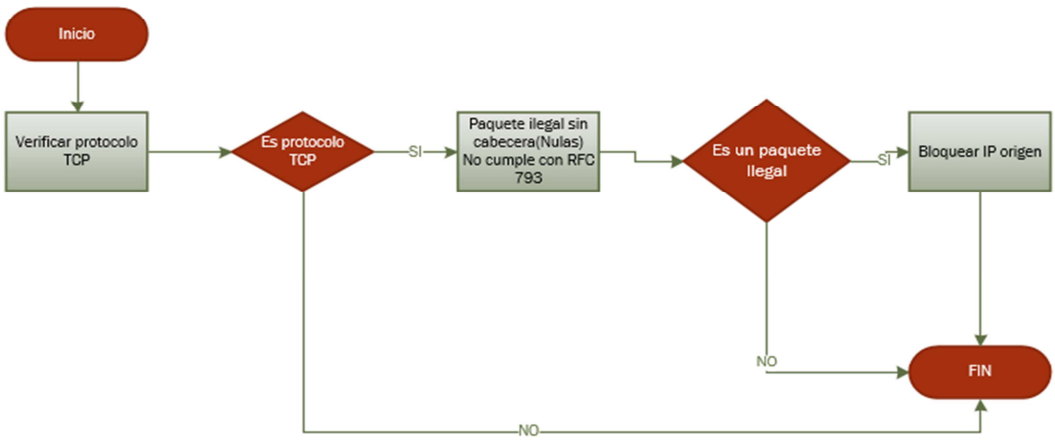

Fig 4.9: Regla Firewall NULL Scan.

Como se puede ver en las figuras 4.10 y 4.11, se puede observar que gran cantidad de paquetes enviados no han llegado a su destino y que el equipo 192.168.0.10 atacante interno ha sido bloqueada por el IDS, lo que significa que el Firewall con el IDS mitiga el escaneo de puertos ya que los administradores suelen crear reglas bloqueando ciertos servicios y paquetes en red, la manera de bloquear estos ataques es bloqueando el origen.

La Tabla 4.10, muestra los resultados obtenidos con la herramienta Wireshark, después de implementar las regla para el ataque TCP descrita anteriormente, de igual manera que en la línea base, se muestra la tabla con paquetes, tiempos de retardo, tamaños y tiempos de transferencias en tres muestras tomadas durante el ataque.

Tabla 4.10: Resultados TCP Scan Con IDS.

TCP	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25
Paquetes	2300	100	145	130
Tiempo(ms)	7.258	6238,1	4215,2	6.841
paq/seg	0,317	0,016	0,034	0,019
SIZE(Bytes)	214	102	523	761

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

La Tabla 4.11 muestra los resultados obtenidos con la herramienta Wireshark, después de implementar las regla para el ataque UDP descrita anteriormente, de igual manera que en la línea base, se muestra la tabla con paquetes, tiempos de retardo, tamaños y tiempos de transferencias en tres muestras tomadas durante el ataque.

Tabla 4.11: Resultados UDP Scan con IDS.

UDP	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25
Paquetes	3214	300	1004	124
Tiempo(ms	6.502	6.841	7.837	7.426
paq/seg	0,49429	0,043851315	0,128111881	0,016697188
SIZE(Bytes	114	84	65	136

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

La Tabla 4.12 muestra los resultados obtenidos con la herramienta Wireshark, después de implementar las regla para el ataque ACK Scan descrita anteriormente, de igual manera que en la línea base se muestra la tabla con paquetes, tiempos de retardo, tamaños y tiempos de transferencias en tres muestras tomadas durante el ataque.

Tabla 4.12: Resultados ACK Scan con IDS.

ACK	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25
Paquetes	852	200	158	105
Tiempo(ms	2.056,8	2.657,6	2.489,2	2.563,9
paq/seg	0,4142	0,0753	0,0635	0,0410
SIZE(Bytes	295	24	216	233

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

La Tabla 4.13 muestra los resultados obtenidos con la herramienta Wireshark, después de implementar las reglas para el ataque NULL Scan descrita anteriormente, de igual manera que en la línea base se muestra la tabla con paquetes, tiempos de retardo, tamaños y tiempos de transferencias en tres muestras tomadas durante el ataque.

Tabla 4.13: Resultados TCP Scan con IDS.

NULL	192.168.0.1	192.168.0.10	192.168.0.15	192.168.0.25
Paquetes	54	0	0	2
Tiempo(ms)	3.254,0	4.136,7	2.036,4	3.526,7
paq/seg	0,01659	0	0	0,00057
SIZE(Bytes)	134,2	11	124	214

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

4.5- Evaluación de resultados

La Figura 24, muestra el envío de paquetes antes de la implementación de IDS y después de la implementación, 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.

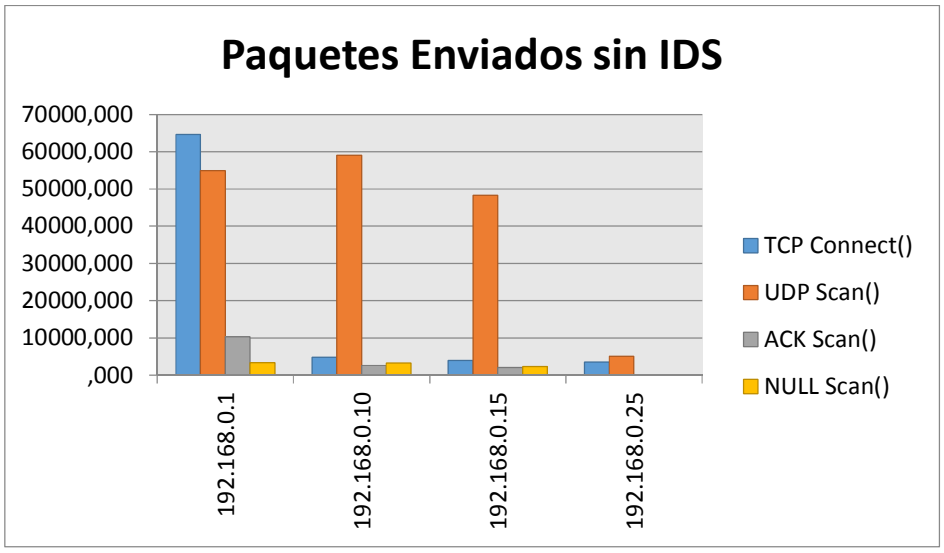

Fig 4.10: Comparación estadistica Envio de Paquetes(Parte1)

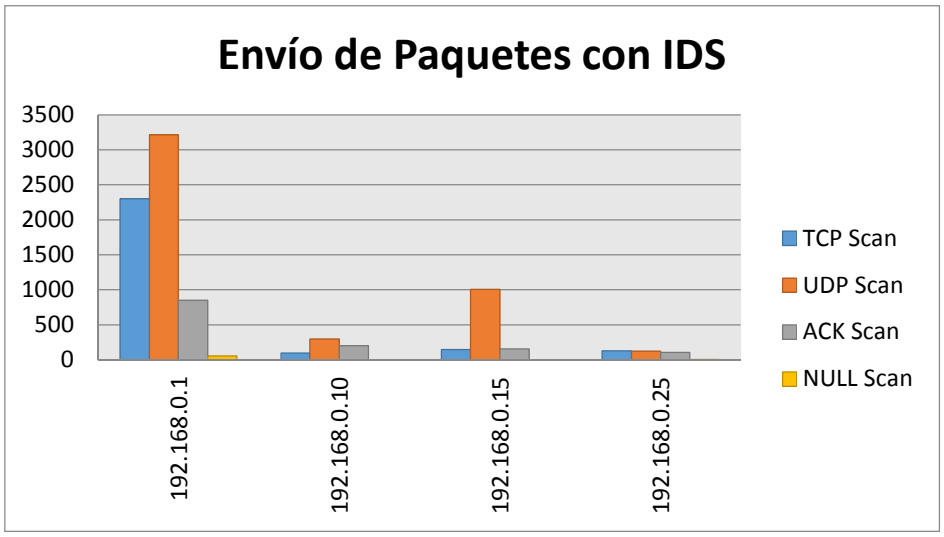

Fig 4.10: Comparación estadistica Envio de Paquetes.(Parte 2)

En cuanto a los tiempos de retardo, como se observa en la Figura 25, 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 la comunicación del atacante hacia las máquinas que componen el laboratorio.

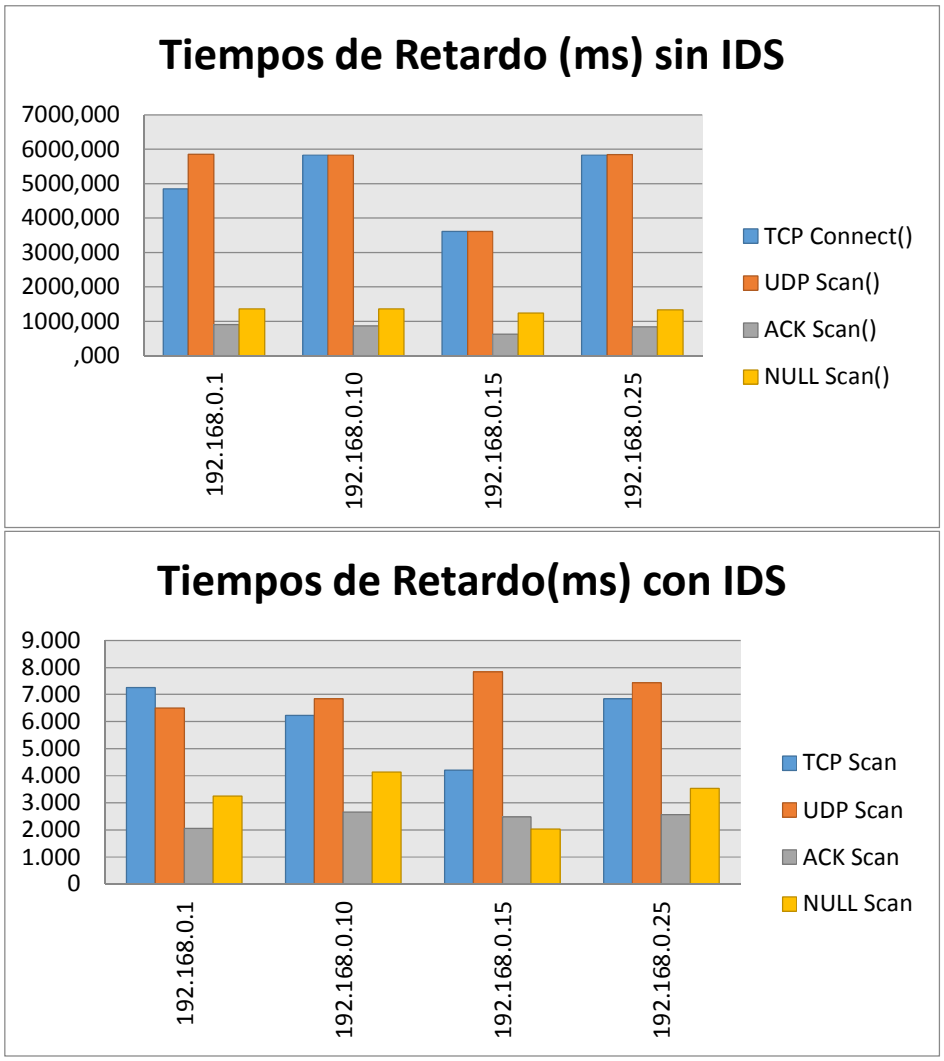

Fig 4.11: Comparación estadística de datos por tiempos.

4.5.1- Discusión

El laboratorio presenta una topología tipo estrella, ya que todos los equipos deben comunicarse por un punto en común en este caso el designado como cortafuegos (Firewall TMG), es el equipo central en esta infraestructura. Por tanto 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 cortafuegos, 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 cortafuego, 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 4.14 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 4.14: 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						

Fuente: Karla Tandazo, Miguel Rueda.

Elaborado: Karla Tandazo, Miguel Rueda

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

- 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 atacantes internos, por lo cual sí se utilizan reglas muy comunes como son las que se han desarrollado. Es necesario un IDS para poder controlar completamente el ataque.
- Como una alternativa se puede 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 es considerado uno de los mejores ya posee la capacidad de aprender patrones de ataque y como se ha demostrado es capaz de bloquear los ataques.
- Este tipo de ataque es exploratorio, por lo cual el enfocarse solamente en bloquear puertos o patrones en los diferentes equipos en la red no es suficiente y no es efectivo, porque lo que buscan estos ataques es encontrar topologías y las puertas para poder ingresar y violentar la infraestructura de red.
- Finalmente, en este trabajo se ha construido un laboratorio para trabajar con ataques de puertos en los cuales se puede experimentar en un ambiente virtualizado y crear diferentes topologías y nuevas reglas que pueden ser aplicadas en muchas empresas ya que es una arquitectura utilizada en gran número de empresas de nuestro país.
- Como resultado del laboratorio se obtienen mejoras en la seguridad en lo que a ataques del tipo TCP se refiere una mejora en seguridad del 96,75%.

- En lo que a ataques de tipo UDP se refiere, la mejora en seguridad evaluada en los paquetes analizados es del 97.27% en relación al análisis inicial.
- En lo que a ataques de tipo ACK se refiere, la mejora en seguridad evaluada en los paquetes analizados es del 91.67% en relación al análisis inicial.
- En lo que a ataques de tipo NULL Scan se refiere, la mejora en seguridad evaluada en los paquetes analizados es del 98.5% en relación al análisis inicial.
- Existe un aumento del 40% en tiempo de retardo, en las comunicaciones del laboratorio virtual, lo cual agrega alrededor de 2 segundos en las comunicaciones debido a la identificación y bloqueo de patrones.

Bibliografía

Open Source Security Testing Methodology Manual. (2010). Obtenido de http://www.isecom.org/research/osstmm.html

Seguridad y Redes. (2010). Obtenido de http://seguridadyredes.nireblog.com/post/2008/03/24/analisis-de-red-con-wireshark-filtros-de-captura-y-visualizacian

Monografías. (2012). Obtenido de http://www.monografias.com/trabajos/hackers/hackers.shtml

27000.org, T. (1 de 04 de 2013). *27000.org*. Obtenido de http://www.27000.org: http://www.27000.org/iso-27004.htm

Anonymous. (2002). *Maximum Security: A Hacker's Guide to Protecting Your Computer Systems and Network, 4th Edition.* USA: Sams.

Carlton, G., & Zhou, H. (16 de 10 de 2011). *A Survey of Cloud Computing.* Obtenido de irma-international.org: http://www.irma-international.org/viewtitle/60237/

Cheswick, W., Bellovin, S., & Rubin, A. (2003). *Firewall and Internet.* Massachuset: Addison Wesley.

CIT. (18 de Noviembre de 2008). *4th International Conference on Innovations in Information Technology.* Obtenido de it-innovations.a: http://www.it-innovations.ae/iit07/index.html

Conference, A. T. (2009). *Australasian Telecommunication Networks and Applications Conference.* Australia.

Corletti, A. (Marzo de 2007). Obtenido de http://www.criptpred.upm.es/guiateoria/gt_m292j.htm

DRAGONJAR. (s.f.). Obtenido de www.dragonjar.org. Obtenido de www.dragonjar.org: http://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

ecualug. (s.f.). *ecualug.org*. Obtenido de http://www.ecualug.org/2012/02/09/blog/epe/curiosidades_de_kvm_ksm

Fernández, D. (2004). *www.rediris.es*. Obtenido de http://www.rediris.es/difusion/publicaciones/boletin/82-83/ponencia1.4A.pdf

Forouzan, B. (2003). *TCP/IP protocol suite 2nd.* Boston: MacGraw Hill.

Fuente, I. R. (2011). *Certificaciones Uruguay*. Obtenido de http://www.cert.uy/historico/pdf/CertificacionesProfesionalesenSeguridaddelaInformacionl.pdf

Fuertes, W., Zambrano, P., Sánchez, M., & Gamboa, P. (2011). *Alternative Engine to Detect and Block Port Scan Attacks using Virtual Network Environments.* International Journal of Computer Science and Network Security.

Gálvez, M. (2006). *Sociabilidad en pantalla Estudio interactivo de entornos virtuales.* Barcelona: UOC.

Galvéz, M. (2006). *Sociabilidad en pantalla: un estudio de la interacción en los entornos virtuales.* Barcelona: UOC.

Garfinkel, S. (2002). *Web Security privacy and commerce 2nd .* Cambridge: O'Reilly.

Hánil, A., & Cantú, J. (2 de 02 de 2013). *http://es.scribd.com*. Obtenido de http://es.scribd.com: http://es.scribd.com/doc/108108070/Tesis-Seguridad-Informatica-Angel-Cantu

Harrison, J. (2010). *Microsoft Forefront threat management gateway (TMG).* Redmond: Microsoft Press.

IEEE. (2005). Symposium on Foundations of Computer Science. *46th Annual IEEE Symposium on Foundations of Computer Science FOCS*, (pág. 1024). Pittsburgh.

ISECOM. (s.f.). Obtenido de www.isecom.org. Obtenido de www.isecom.org: http://www.isecom.org/mirror/OSSTMM.3.pdf

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

Llerena, M., & Saa, J. D. (s.f.). *Espe Repositorio*. Obtenido de http://repositorio.espe.edu.ec/

Lyon, G. (2008). *NMAP Network Scanning .* USA: Fyodor.

Lyon, G. F. (2008). *Nmap network scanning.* USA: Insecure.Com.

Machinery, A. f. (2004). *Internet Measurement Conference.* New York: ACM Press.

nmao. (s.f.). *NMAP*.

NMAP. (s.f.). Obtenido de http://nmap.org.man/es

Northcutt, S., Judy, N., & Donald, M. (2000). *Network Intrusion Detection.* USA: New Riders Publishing.

Orebaugh, A. (2007). *Wireshark and Ethereal Network Protocol Analyzer Toolkit .* USA: Elsevier Science.

Peláez, R. (1 de Junio de 2002). *Análisis de Seguridad de la familia de protocolos TCP/IP y sus servicicos asociados*. Obtenido de sisman: http://www.sisman.utm.edu.ec/libros/FACULTAD%20DE%20CIENCIAS%20IN

FORM%C3%81TICAS/CARRERA%20DE%20INGENIER%C3%8DA%20DE%20SISTEMAS%20INFORMATICOS/06/Administraci%C3%B3n%20de%20Redes/Seguridad_en_TCP-IP_Ed1.pdf

Quétier, B., & Cappello, F. (01 de 01 de 2013). *link.springer.com.* Obtenido de link.springer.com: http://link.springer.com/content/pdf/10.1007/s10723-006-9052-6.pdf#page-1

Rash, M. (2007). *Linux firewalls.* San Francisco: No Starch Press.

Rash, M. (2007). *Linux Firewalls attack detection and response with iptables.* San francisco.

Scambray, J. (2001). *Hacking Exposed network security secrets and solutions 2nd.* USA: Osborne-McGraw Hill.

Scott, C. (1999). *Virtual private networks (2nd ed.).* Beijing: O'Reilly.

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

Society, N. A. (2000). *International Conference of the North American Fuzzy Information Processing Society.* Atlanta Georgia: Piscataway.

Vincosoft. (s.f.). Obtenido de http://www.vincomsoft.com/learning-center/pppop

Wireshark. (s.f.). Obtenido de http://seguridadyredes.nireblog.com/post/2010/03/24/wireshark-tshark-capturando-impresiones-en-red

WIreshark. (s.f.). Obtenido de http://seguridadyredes.nireblog.com/post/2010/03/24/wireshark-tshark-capturando-impresiones-en-red

Workshop, A. (2007). *Proceedings of the 2007 Workshop on Experimental Computer Scienc.* San Diego: ACM Press.

Nombre: Miguel Angel Rueda Salgado

Nacionalidad: Ecuatoriana

Lugar de nacimiento: Quito

Fecha de nacimiento: 4 de Mayo del 1986

Instrucción Primaria

Nombre: Unidad Educativa Borja No 3.
Período: 1992-1998

Instrucción Secundaria

Nombre: Unidad Educativa Jean Jacques Rousseau
Período: 1998-2004
Título: Bachiller en Ciencias (2004)

Certificaciones

- IBM Certified Advanced Deployment Professional in IBM Monitoring 6.2
- IBM Certified Deployment Professional for OMNIBus v7.3
- Certificación Desarrollador 5 estrellas Microsoft
- Professional GIS Developer Flex Applications by ESRI
- Professional GIS Developer Silverlight Applications by ESRI

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR

_____

Karla Cecibel Tandazo Jimenez

_____

Miguel Ángel Rueda Salgado

DIRECTOR DE LA CARRERA

_____

Ing. Mauricio Campaña

Sangolquí, Agosto de 2013