ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

INSTITUTO DE POSGRADO Y EDUCACIÓN CONTINUA

FRAMEWORK EN ESTRUCTURAS CON DIRECCIONAMIENTO IPV6 SOBRE OSSTMM PARA LA CORRECIÓN DE VULNERABILIDADES DE SEGURIDAD EN UN LABORATORIO DE LA ACADEMIA CISCO DE LA ESPOCH

Proyecto de Investigación, presentado ante el Instituto de Postgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de

MAGÍSTER EN SEGURIDAD TELEMÁTICA

AUTOR: CARLOS JOSE MARTINEZ SANTANDER

Riobamba-Ecuador

Diciembre-2015

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

INSTITUTO DE POSGRADO Y EDUCACIÓN CONTINUA

El Tribunal de Proyecto de Investigación certifica **Framework en estructuras con direccionamiento ipv6 sobre osstmm para la corrección de vulnerabilidades de seguridad en un laboratorio de la academia CISCO de la ESPOCH,** de responsabilidad de Carlos José Martínez Santander, ha sido minuciosamente revisado por los Miembros del Tribunal de investigación, quedando autorizada su presentación.

Ing. William Pilco Mosquera .Mgs. **PRESIDENTE**	FIRMA
Ing. Hugo Moreno Avilés .PhD. **DIRECTOR**	FIRMA
Ing. Verónica Mora Chunllo .Mgs. **MIEMBRO**	FIRMA
Ing. Wilson Baldeón López .Mgs **MIEMBRO**	FIRMA
DOCUMENTALISTA **SISBIB ESPOCH**	FIRMA

Riobamba – Ecuador
2015

Yo,**Carlos José Martínez Santander** soy responsable de las ideas, doctrinas y resultados expuestos en la presente Investigación, el patrimonio intelectual generado por la misma pertenece a la **Escuela Superior Politécnica de Chimborazo.**

_____

Carlos José Martínez Santander

DEDICATORIA

En primer lugar al todo poderoso Dios que me ayudado con la culminación de una etapa más de mi vida, a mi madre amada, **María Santander** que con su esfuerzo apoyo ha hecho de mi un hombre de bien, a mi hermana por estar siempre en los momentos fáciles y difíciles de mi vida, a mis **hijos Carla, Pancho y Jackson** que soy su ejemplo a seguir.

Carlos

AGRADECIMIENTO

Gracias a Dios por guiarme en este duro camino, al Doctor Hugo Moreno, Ing. Verónica Mora, Ing. Wilson Baldeon, que me han guiado con su sólido conocimiento en la realización de este trabajo. A todas las personas que de una y otra manera me han apoyado en este proceso, un eterno agradecimiento a todos.

Carlos

ÍNDICE

INDICE DE TABLAS

N°CONTENIDO **Pagina**

INDICE DE FIGURAS

RESUMEN

Seelaboró una propuesta para realizar un Framework en estructuras con direccionamiento IPv6 sobre Open Source Security Testing Methodology Manual (OSSTMM) para la corrección de vulnerabilidades de seguridad en un laboratorio de Academia Local de redes (CISCO) de la Escuela Superior Politécnica de Chimborazo.Se recopilo tendencias sobre vulnerabilidades de seguridad, además de una experimentación, análisis y aplicación, para solucionar errores de seguridad en arquitecturas IPv6; Este trabajo se basó en la metodología OSSTMM y se dividió en tres fases:1) Análisis y evaluación de riesgos en arquitecturas IPv6. 2) Identificación y búsqueda de vulnerabilidades en IPv6. 3) Informe, valoración y posibles tratamientos para evitar que existan vulnerabilidades de seguridad en la arquitectura Ipv6. El análisis de los resultados demostró que el framework corrige las vulnerabilidades en un 70,60% brindando mayor seguridad y conocimiento sobre los ataques que pueden afectar la infraestructura de los protocolos versión 6 en un laboratorio de CISCO. Se concluye que es imprescindible un framework para un análisis rápido y veraz de una arquitectura IPv6 para establecer una estrategia que profundice el tema de seguridad en arquitectura versión 6. Para futuros trabajos se sugiere continuar en la búsqueda de soluciones de vulnerabilidades que no están corregidas en esta.

Palabras claves:<MARCO DE TRABAJO>< PROTOCOLO DE INTERNET VERSIÓN 6><MANUAL DE METODOLOGIA DE PRUEBAS ABIERTAS PARA SEGURIDAD (OSSTMM)>< ACADEMIA LOCAL DE REDES (CISCO)>< VULNERABILIDAD><SEGURIDAD TELEMÁTICA><INFORMATICA APLICADA>

SUMARY

A proposal was made for a Framework on IPv6 routing structures Open Source Security Testing Methodology Manual (OSSTMM)) to correct security vulnerabilities in a laboratory of the Local Networking Academy (CISCO) of the Higher Polytechnic School of Chimborazo.Trends on security vulnerabilities, along with a testing, analysis and application were collected to troubleshoot IPv6 security architectures. This work was based on the OSSTMM methodology and was divided into three phases: 1) Analysis and Risk Assessment IPv6 architectures. 2) Identification and search for vulnerabilities in IPv6 3) Report, evaluation and possible treatments to prevent security vulnerabilities exist in the IPv6 architecture.The analysis of the results showed that the framework address the vulnerabilities on a 70.60% providing greater security and knowledge of attacks that may affect the infrastructure of the protocol version 6 on a CISCO laboratory. It is concluded that a framework is essential for fast and accurate analysis of IPv6 architecture to establish a strategy that deepens the security issue in version 6architecture. For future work it is suggested to continue in the search for solutions that are not corrected vulnerabilities in it.

KEYWORDS: <FRAMEWORK>,< INTERNET PROTOCOL VERSION 6 >,< OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) >, <LOCAL NETWORKING ACADEMY (CISCO)>, < VULNERABILITY>,<SECURITY TELEMATIC>, <APPLIED COMPUTATION>

CAPITULO I

1. INTRODUCCIÓN

Al hablar de seguridad de la información involucra una serie de metodologías, conceptos, mecanismos, herramientas y procedimientos que se investigan para asegurar todos los sistemas informáticos que implican datos, equipos y dispositivos, la seguridad es un proceso que se considera como el eslabón más débil de un sistema informático.

Los equipos de cómputo nunca estarán protegidos al 100%, porque por más esfuerzos que los técnicos le den siempre existirán pequeños agujeros que se los pueda comprometer y la idea de esta investigación es llegar a buscar una aproximación lo más cercana posible a un aseguramiento eficaz.

La seguridad es una batalla continua entre el atacante y el administrador de los sistemas; los atacantes lo que aprovechan son las vulnerabilidades para alcanzar una penetración mientras que el administrador tiene que utilizar blindajes en contra de todas las vulnerabilidades en su contra ya sean existentes o por existir.

La implantación de seguridad generalmente colisiona con la eficiencia puesto que no es recomendable poner varios controles o mecanismos que protejan la información por el simple hecho de que se vuelven ineficientes , además se debe tener en cuenta costo beneficio de acuerdo a la organización que requiera del servicio de seguridad.

Las motivaciones de los atacantes hoy en la actualidad han cambiado debido a que lo hacen por obtener ganancias económicas es decir motivación monetaria, si hablamos de unos años atrás lo hacían por juego o prestigio queriendo demostrar que eran mejores que los administradores o encargados de la seguridad de una empresa . existen organizaciones dedicadas a las actividades de seguridad como son CSI Computer Crime and Security Survey que trabaja activamente en el mejoramiento de la seguridad para dar servicio a empresas que han sido víctimas de los hackers, esta organización dio a conocer que los incidentes más comunes son accesos no autorizados, denegación de servicios, abuso de mensajería instantánea, virus, robo de laptops, y otros incidentes

relacionados son abusos de redes inalámbricas, penetración a sistemas, ataques a DNS, mal uso de aplicaciones web etc.

En cuanto a ataques las vulnerabilidades más utilizadas son la de inyección SQL, Cross site Scripting, autenticación y anti-automatización insuficiente, («SEGURIDAD INFORMÁTICA», 2002)

Dado a conocer la situación de inseguridad que presenta IPv6 la investigación se centra en buscar errores y mitigar sus vulnerabilidades con la metodología OSSTMM en el departamento de CISCO de la Escuela Superior Politécnica de Chimborazo.

1.1 Problema de investigación

1.1.1 *Planteamiento del problema*.

Son ya cuatro décadas en las que se inventaron los servicios en la redcon esta invención las estructuras jerárquicas en la red son aún más complejas(WANG YI D, FAN JIAN B, PAM PUI C, & LAM D, 2008, p.2). Varias fueron las empresas y entidades públicas, privadas que volcaron sus aplicaciones al uso de estos servicios(JAIMES SANTOS L & BAUTISTA W, 2007,P.415-416),es así que se estima que 680.000.000 sitios web han sido creados, 300.000.000 hasta el año al 2011 y 380.000.000 al 2014. Redes Sociales tienen ya 1000.000.000 usuarios que intercambian millones SMS en el día por medio de otros sistemas de comunicación (WhatsApp), por tal motivo los servidores de correo y web deben contar con direcciones fijas o estáticas para saber su ubicación (THOMSON BELLCORE S & NARTEN T, 1998,p. 1-20)

Según Núñez Lara, 2009 con el transcurso del tiempo y con la aparición de nuevas tecnologías, son varios los protocolos que comandan la nueva era tecnológica con mayor capacidad de trasmitir información mayor velocidad y seguridad, IPV4 por ejemplo ha llegado a agotar las direcciones IP disponibles lo que genera que los usuarios usen NAT,(ESPINOSA C, MALDONADO D, VALAREZO C, CARRASCO P, & BARRERA J, 2004, p. 8)

IPv6 se creó para Ipv4 nació en los 98 por la IETF (The Internet Engineering Task Force), mayores tareas y más direcciones.

Diversas, son las redes de telecomunicaciones que han manifestado sus estudios sobre estructuras con direccionamiento IPV6 (CHOUDHARY A & SEKELSKY A, 2010,p. 5); es así que, la red de Información Global (GIG) para el Departamento de Defensa (DoD) y el OneNet para el Departamento de Seguridad Nacional por el Departamento de Defensa CIO Memorando de Junio de 2003 y la Oficina de Gestión y Presupuesto memorando OMB-05-22, existen IPv6,(GHEBREGZIABHER T, PUTTONEN J, HAMALAINEN T, & VIINIKAINEN A, 2006, p. 5-10)Y han destinado su transición hacia el protocolo de Internet versión seis (6) (IPv6) con vulnerabilidades de seguridad específica.

En estas infraestructuras de red que deben ser mitigados con el fin de lograr la paridad de seguridad con las operaciones IPv4 existentes, desde la perspectiva de las tecnologías de la Seguridad Nacional, la existencia de vulnerabilidades de seguridad adicionales implica la posibilidad de que dos amenazas: En primer lugar, las vulnerabilidades específicas IPv6 reducen la postura de seguridad de la infraestructura de la red en sí; segundo, otros sectores de infraestructuras críticas que dependen de IPv6 necesitan protección adicional .

Se han realizado investigaciones sobre seguridad informática revelando que existe un aumento de actividadesilícitas por parte de personas que a través ataques cibernéticos engañan otras ya sea mediante la publicación de sitios web maliciosos, falsificaciones de empresas legítimas y campañas de spam (GEROMETTA O, 2007, p. 1).

Los frameworks aplicados a protocolos IPv6 tienen como punto fundamental corregir errores de seguridad, se debe tomar como referencia que los ataques efectuados en la versión 4 no servirán en la versión 6, para asignar direcciones unicast a este protocolo se deben buscar caminos que me conlleven a las EUI-64 Extended Universal Identifier (EUI)a través de RFC 2464 con identificador de 64 bits,(GERRERO POLICIA CIBERNETICA, 2014,p.1)

1.2 Formulación del problema

¿Cómo corregir las vulnerabilidades de seguridad en las estructuras con direccionamiento IPv6 sobre OSSMTT?

1.3 Sistematización del problema

1. ¿Cuáles son las aplicaciones de frameworks históricos para la reducción de vulnerabilidades de seguridad en las estructuras IPv6 en Ecuador?

2. ¿Cuáles son los fundamentos teóricos generales que sirven de sustento al estudio de la vulnerabilidad de seguridad en las estructuras con diferentes direccionamiento con énfasis en el IPv6?

3. ¿Qué procedimientos técnicos se deben seguir para reducir la vulnerabilidad de seguridad en las estructuras con direccionamiento IPv6?

3. ¿Cómo valorar la factibilidad del procedimiento propuesto?

1.4 Justificación

Teórico

Existe un estudio similar en estructuras con direccionamientos utilizando la metodología OSSTMM en la Escuela Politécnica Nacional de la ciudad de Quito se basa en la búsqueda y verificación de vulnerabilidades identificación y testeo de aplicaciones, su procedimiento se basa en 2 pasos sencillos el primer paso hace relación a las pruebas de rastreo y el segundo paso a las pruebas de intrusión basadas en el marco referencial de la metodología OSSTMM(COELLO M, 2013, p.1-10).

Para obtener resultados satisfactorios se utiliza un análisis de requerimientos de seguridad basados en la metodología vigente, utilización de los requerimientos de la normativa dividida en secciones, se analizara las vulnerabilidades ya existentes en los sistemas y especificarlas en la metodología OSSTMM.

Como resultados obtuvieron en realizar cambios a la normativa que afectan las políticas internas y externas de seguridad del lugar en análisis, proponer guías de control para medir el nivel de vulnerabilidad, la variante que tendrá este estudio será centrarse a un Framework en estructuras con direccionamiento IPV6 sobre OSSTMM para la corrección de vulnerabilidades de seguridad en un laboratorio de la academia CISCO de la Espoch.

Para solucionar el problema de corrección de vulnerabilidades como primer paso sería identificar enemigos, vulnerabilidades y amenazas en la estructura de los protocolos IPv6. Primero, para detectar los enemigos se explorara el análisis del modelo de seguridad OSSTMM. Segundo para detectar las vulnerabilidades se examinara las que se puedan presentar en la estructura del protocolo IPv6 y determinar cada amenaza.
Se espera obtener resultados de la detección de las vulnerabilidades como un listado de las vulnerabilidades de autenticación encontradas y asociarlas en un laboratorio de la academia CISCO de la ESPOCH, reducir los falsos positivos, falsos negativos, errores humanos, puertos abiertos (direcciones IP, servicios, tipos de servicios activos), nivel de parchado rastreo de red.

Metodológica

La metodología a seguir en la investigación tiene incidencia directa en la metodología OSSTMM (Manual de la metodología Abierta de Testeo de Seguridad) versión 2.1, que se detallara en el desarrollo del Framework. OSSTMM (Open Source Security Testing Methodology Manual) o "Manual de la Metodología Abierta de Testeo de Seguridad" tal como fue nombrada oficialmente su versión en español, es un manual aplicable a las pruebas de seguridad informática de una empresa privada u organización gubernamental.

En el año 2001fue creada por Pete Herzog, Director Ejecutivo de ISECOM (Instituto para la Seguridad y Metodologías Abiertas), la metodología de seguridad incluye fases, módulos, test. El OSSTMM contempla seis tipos de test.

• Blindaje o Hacking Ético.

- Doble blindaje, auditoría de Caja Negra o Pruebas de Penetración.
- De Caja Gris.
- De Doble Caja Gris.
- Test Tándem o Secuencial.
- Inverso

La metodología se divide en ambientes para el análisis de seguridad por secciones. **VER Figura 1-1**

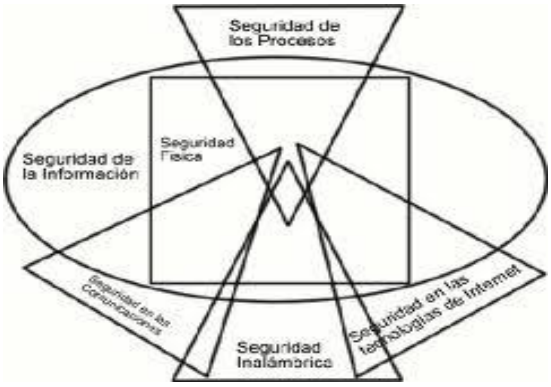


Figura 1-1 Sección del manual OSTMM
Fuente:**(HERZOG PETE, 2003)**

La sección C del manual OSSTMM, se utilizara para la presente investigación, se enfocara en la seguridad de los protocolos de la seguridad de la información se partirá por etapas para el desarrollo de la investigación: descripción, análisis y corrección de los requerimientos del procedimiento.

Practico

Basándonos en la metodología referenciada anteriormente se hará un test de seguridad usando software especialista en esto; primero será necesario verificar si las vulnerabilidades persistentes en IPv4 también se encuentran en IPv6, después se explotara vulnerabilidades exclusivamente de IPv6, después de buscar nuevas maneras de vulnerar esta estructura; todo esto permitirá recopilar datos para hacer un informe que a su vez comparando con otros resultados y con estudios anterior se elaborara una FRAMEWORK con los resultados obtenidos. A continuación se explica a groso modo como trabaja la metodología OSSTMM que plantea categorizaciones estándar, permiten

identificar claramente el alcance de cada una de las actividades, evitando inconvenientes en tal sentido:

- **Búsqueda de Vulnerabilidades:** indagación de debilidades utilizando herramientas tecnológicas dentro de una red.
- **Escaneo de la Seguridad:** Encaminado a encontrar los puntos débiles en el sistema
- **Test de Intrusión:** son test que sirven para romper la seguridad de un sistema determinado.
- **Evaluación de Riesgo:** Valora la seguridadutilizando diversos instrumentos de investigación.
- **Auditoria de Seguridad***:* revisión del sistema por medio del auditor interno o externo para verificar si son implantadas las políticas de seguridad.
- **Hacking Ético***:* obtiene las vulnerabilidades y errores que tiene un sistema para reportarlo y corregirlo.

1.5 Objetivos

1.5.1 General

Desarrollar un Framework en estructuras con direccionamiento IPV6 sobre OSSMTT para la corrección de vulnerabilidades de seguridad en el Laboratorio de CISCO de la Espoch.

1.5.2 Específicos

- Recopilar las tendencias e históricos de aplicación del estudio de la reducción de la vulnerabilidad de seguridad en las estructuras con diferentes direccionamiento, con énfasis en el IPV6.
- Determinar los indicadores de vulnerabilidad de seguridad en IPV6.
- Implementar procedimientos de detección de errores para reducir la vulnerabilidad de seguridad en las estructuras con direccionamiento IPV6.
- Validar los indicadores de la metodología OSSMTT sobre el framework.

1.6 Hipótesis

¿Es posible corregir la vulnerabilidad de seguridad en las estructuras con direccionamiento IPV6 a través del desarrollo de un Framework?

CAPITULO II

2. MARCO DE REFERENCIA

Cuando se identifica vulnerabilidades es decir debilidades que violentan la confidencialidad, integridad y disponibilidad de información por parte de los atacantes a los protocolos de red como es el caso de IPv6 que es la versión 6 de los protocolos de internet, son puntos frágiles para que los hackers ataquen los puntos inseguros de la red.

Se han realizado investigaciones sobre seguridad informática,(LA FLECHA DIARIO DE CIENCIA Y TECNOLOGIA, 2008, p1) revelando que existe un aumento de actividades ilícitas por parte de personas que a través ataques cibernéticos engañan otras ya sea mediante la publicación de sitios web maliciosos, falsificaciones de empresas legítimas, campañas de spam.

La nueva tecnología que surgió debido al agotamiento de las direcciones IPv4, es el direccionamiento IPv6, misma que al ser nueva tecnología, trae consigo muchos problemas de seguridad igual a los de IPv4 o nuevos, problemas que aparecerán ya con el uso en las estructuras de las entidades que son blancos de los hackers.

2.1 IPv6

En la década de los 80 Ipv4 se lanzó a nivel mundial y no se realizó ningún cambio ni actualización, aproximadamente son 35 años de utilizar este tipo de protocolo mostrando que es flexible, robusto(DURDA E & BULDU A, 2010,p. 3-7). Pero desde años atrás cerca del año 2007 ha comenzado a mostrar un crecimiento exponencial de internet que está llevando hacia un agotamiento en las direcciones IPv4, es decir comenzó a evidenciarse la progresiva disminución de la cantidad de direcciones IPv4 disponibles para cubrir la gran demanda generada este agotamiento ha sido de suma preocupación, (JAIMES SANTOS L & BAUTISTA W, 2007, p. 10-20). Las limitaciones presentadas por Ipv4 comenzaron a mostrar problemas de conciliación al funcionamiento de las redes actuales y futura demandas ; creadores del protocolo Ipv4 no previnieron el crecimiento a pasos agigantados de las redes y la evolución de la tecnología que es a diario, sin

tomar en cuenta que se debía fortalecer puntos importantes como es la seguridad.

Con la carencia de direcciones y con las actualizaciones diarias en las tecnologías llevaron a crear nuevas versiones en los protocolos de direccionamiento es así que aparece en elaño 2002 nuevas condiciones como es IPv6 que su objetivo era solucionar los problemas que acogían y presentaba IPv4, como extender en un número considerable las direcciones IP de 128 bits, en vez de las direcciones de 32 bits de IPv4 y seguridad sobre la capa de Red, cuenta con las siguientes características:**VER TABLA 1-2**

Tabla 1-2 Razones para migrar de IPv4 a IPv6

CARACTERÍSTICAS QUE CONLLEVO AL PROTOCOLO IPv4 MIGRAR A IPv6	
IPv4	**IPv6**
• El agotamiento de direcciones Ipv4	• Espacio de direcciones más grande (128 bits)
• Mantener tablas de ruteo largas	• Formato de cabecera simplificado
• Inexistencia de una configuración simple de direccionamiento	• Direccionamiento e infraestructura de ruteo eficiente y jerárquica
• La no existencia de métodos para él envió de tráfico en tiempo real (QoS	• Configuración de direcciones con y sin estado.
• Falta de seguridad en la red	• Seguridad intrínseca en el núcleo del protocolo
• Falta de soporte	• Mejor soporte para la Calidad de Servicio
• Sin protocolo de interacción	• Nuevo protocolo para la interacción entre nodos vecinos
• Sin extensibilidad	• " Extensibilidad
	• Multicast (envió un mismo paquete a un grupo de receptores)
	• Anycast (envió de un paquete a un receptor dentro de un grupo)
	• Posibilidad de enviar paquetes con más de 65.535 bytes (jumbogramas)
	• Remuneración y multi-homing, que facilita el cambio de proveedor de servicios de Internet
	• Características de movilidad"

Realizado por: Martínez, Carlos, 2015

El motivo de la presente investigación se desarrolla para encontrar los errores y solucionar vulnerabilidades de seguridad del protocolo IPv6, lo cual brindara una estrategia y metodología que si bien no brinda la solución total se podrá cubrir parte de los agujeros que hoy presenta al hablar de seguridad informática.

Steve Deering de Xerox PARC y Craig Mudge son los investigadores y diseñadores de IPv6, era una versión que reemplazaría a Ipv4 debido a desventajas que comenzaron a surgir en IPv4, como el termino de direccionamientos, problemas de enrutamiento y su configuración en la red,y comienzan a ver los beneficios de estas desventajas como a extender el número de bits para el direccionamiento, a retirar algunos campos que estaban de más en IPv4, mejoran la velocidad de ejecución. Con la actualización tecnológica en países asiáticos,el gobierno de la revolución ciudadana en diciembre del 2011 a través de la asamblea constituyente por decreto impone la ejecución de políticas públicas, que el ministerio de telecomunicaciones y de la Sociedad de la información disponga de acciones para la transición de Ipv4 aIPv6, a entidades públicos y privadas,(COELLAR J & CEDEÑO J, 2013, p.)

Para salir IPv6 había otras versiones que trataban de solucionar los problemas que aquejaban a IPv4, IPng o IPv6 hoy en día da mayor elasticidad y mejora soluciones.
Los principios que debe seguir IPv6 son: **VER TABLA 2-2**

Tabla 2-2 Principios básicos de IPv6

PRINCIPIOS BASICOS DE IPv6
• Superar direcciones IPv4 actuales. • Disminuye el número de las tablas de enrutamiento. • No existen campos innecesarios para que su enrutamiento sea más rápido • Contar con la máxima privacidad • Servicios dedicados al tráfico en tiempo real. • Proveer mayor transmisión a destinos múltiples, y ver su tamaño. • Movilizar un equipo sin cambiar su dirección. • Permitir el desarrollo del protocolo. • Compatibilidad de IPv4 e IPv6.

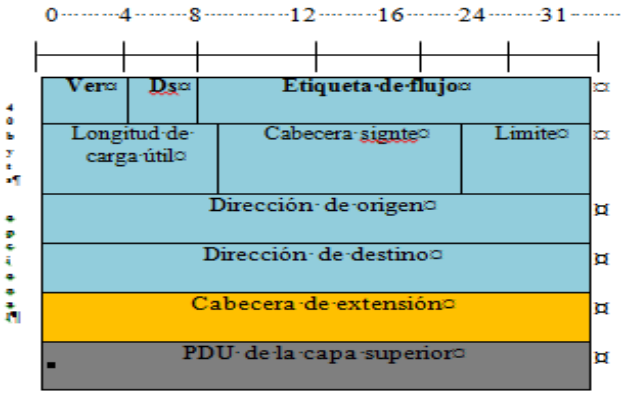
Realizado por: Martínez, Carlos, 2015

2.2 Arquitectura del protocolo IPv6

La arquitectura IPv6formada por 40 bytes fijos en su cabecera, una extensión opcional que no es adicionada a la cabecera fija, tal como se observan en la **Tabla 3-2**
La estructura IPv6 se basa en las cabeceras cuyas particularidades se deben:

1. En la extensión de direcciones incremento a 128 bits cada dirección.
2. IPv6 opera con longitud fija.

Tabla 3-2 Datagrama de IPV6



Fuente: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf)

Versión mejorada el doble de cabecera, por tamaño en los campos "Dirección de origen" y "Dirección de destino".

En la tabla 4-2 se muestra las cabeceras con las que cuenta IPv6:

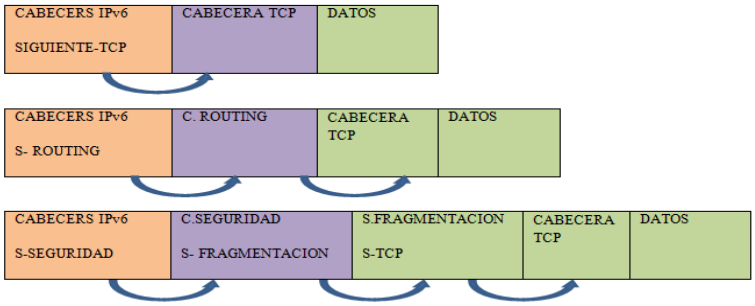
Tabla 4-2 Cabeceras IPv6

Version Muestra el número de versión del protocolo)	**Dos** Prioridad o clase, TOS de IPv4, su longitud es de 8 bits (4 bits).	**Etiqueta de flujo** Soporta tráfico en tiempo real de 24 bits.
Longitud de carga útil Longitud de los propios datos, cuya longitud es de 16 bits, ósea, 2 bytes.	**Cabecera siguiente** Emplea sucesivas cabeceras encadenadas, de ahí que desapareció el campo de opciones, cuya longitud es de 4 bits (1 byte).	**Límite de saltos** Saltos 8 bits (1 byte).
Dirección de origen Envía el paquete de datos de 128 bits.		
Dirección de destino Recibe todos los datos de 128bits		
Cabecera de extensión Proporcionaencaminamiento y fragmentación , opciones de Seguridad		
PDU de la capa superior PDU superior suele constar de un encabezado de protocolo de nivel superior y su carga (por ejemplo, un mensaje ICMPv6, un mensaje UDP o un segmento TCP).		

Realizado por: Martínez, Carlos, 2015

TABLA 5-2, muestra las fases delas cabeceras y sus respectivas correspondencia, es decir, observa los mecanismo en cada cabecera que se "encadenada" a la siguiente.

Tabla 5-2 Extensiones de cabecera



FUENTE: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf

La **Figura 1-2** da a conocer que existen fluctuaciones en los dos protocolos, en las que se pueden observar que cada protocolo tiene su versión y eso no cambia, y se puede apreciar que ciertos campos desaparecieron es así como longitud de cabecera, Tos, identificador, Flags etc. Existe robustez de campos en la longitud, tiempo de vida y protocolos,(ROBLES M, 2008, p. 2-4)

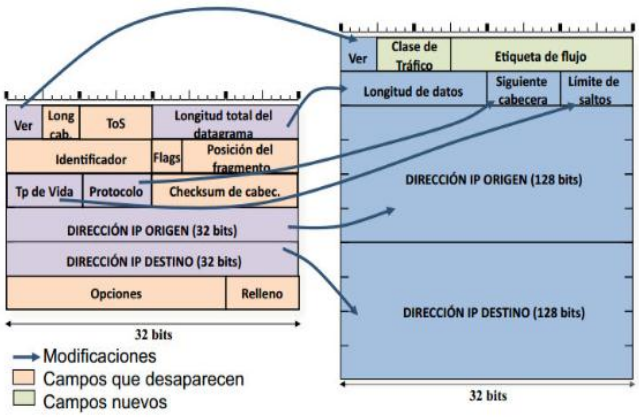


Figura 1-2 Semejanzas de los protocolos IPv4 e IPv6
Fuente: http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf

Tabla 6-2 Valores asignados para encabezados IPv6

Valor (10)	Abreviatura	Explicación
0	HBH	Opciones entre saltos
4	IP	IP e IP (encapsulación en Ipv4)
5	ST	Flujo
6	TCP	Protocolo de control de transmisión
17	UDP	Protocolo de datagrama de usuario
51	AH	Autenticación de encabezamiento
52	ESP	Encriptación de seguridad de la carga útil
59	NULL	No próximo encabezamiento
60	DO	Opciones de destino del encabezamiento
194	JBGR	Jumbo Gram

FUENTE: http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf

Como lo indica (VERDEJO ALVAREZ G, 2009,p.1) el orden de los encabezados dependiendo de su importancia son los siguientes: **VER TABLA 7-2**

Tabla 7-2 Jerarquías del protocolo IPv6

ORDEN	ENCABEZADOS
1	Encabezado (IPv6 Header).
2	Encabezado entre saltos (Hop-by-hop Options Header).
3	1ro encabezado de opciones de destino (Destination Options Header).
4	Enrutamiento (Routing Header).
5	Fragmentación (Fragment Header).
6	Autenticación (Authentication Header).
7	2do encabezado de opciones de destino (Destination Options Header).
8	Protocolo de nivel superior (TCP, UDP).

Realizado por: Martínez, Carlos, 2015

2.2.1 Tipos de protocolos IPv6

IPv6 reconoce las interfaces individuales o grupales, las direcciones se las numera de forma hexadecimal ya que su longitud es de 128 para separar y se corte la dirección se pone dos puntos y si existen más grupos de ceros se toma cuatro, IPv6define el prefijo de red, identificación de subred y de la maquina como que se muestra en la **Figura 2-2:**

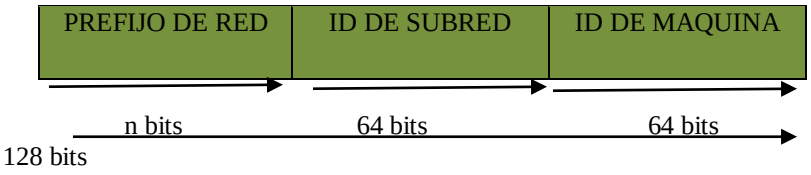


Figura 2-2 Campos que conforman las direcciones IPv6
Fuente: http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf

IPv6de acuerdo al prefijo se divide en: Unicast, Anycast y Multicast.

2.2.2.1Únicast**.-**como su nombre lo dice comunicación de una sola vía, configuración automática, tal como muestra la Figura **4-2**

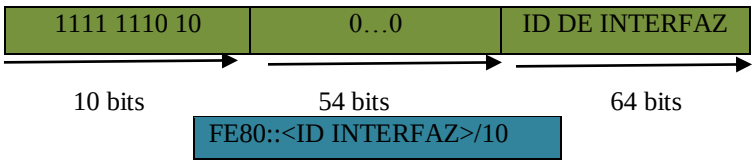


Figura 3-2 Direccionamiento (Unicast) local de enlace
Fuente: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf)

El direccionamiento Unicast está formado por tres campos como muestra la Figura **4-2**

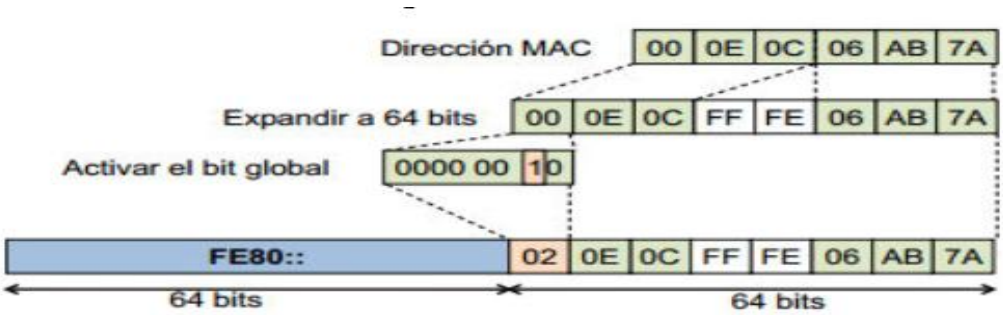


Figura 4-2 Direccionamiento (Unicast) local de enlace Ethernet
Fuente: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf)

La **Figura 5-2** muestra como envía paquetes desde la Pc transmisora a varias Pcs receptoras pero como el direccionamiento de IPv6 es unicast el paquete tomara una sola vía es decir una sola pc receptora.

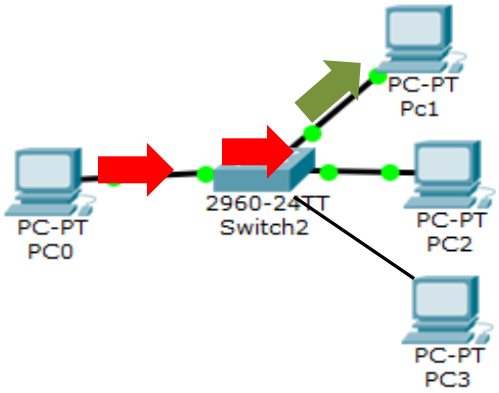


Figura 5-2 Direccionamiento Unicast
Fuente: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf)

2.2.2.2 *Anycast*

Es un direccionamiento donde los datos buscan el mejor enrutamiento para su destino tomando en cuenta su topología, crea copias de tráfico para el peor escenario que caiga la primera máquina , anycast se entregan a una sola interfaz, de un grupo la dirección anycast como <<uno>> a <<uno-entre-muchos(HORLEY E, 2014,p. 17)**Ver Figura 6-2**

.

Figura 6-2 Direccionamiento (Anycast) de los routers
FUENTE: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf)

Ayuda a disminuir los ataques distribuidos puesto que el tráfico es envido al nodo más cercano y esta acción no puede controlar el atacante, seguridad en el redireccionamiento

de paquetes para no ser víctimas del ataque man-in-the –middle, más fiable ya que se recupera fácil a fallos de máquinas (PALET J, 1999, P.12-15)

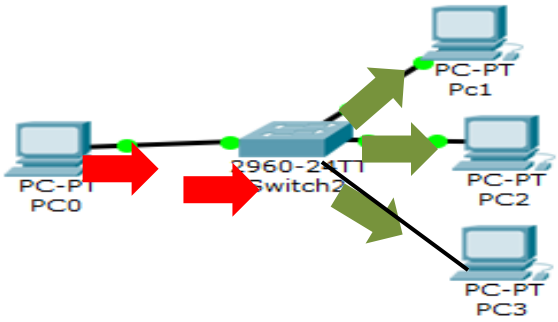


Figura 7-2 Direccionamiento Anycast
FUENTE: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf)

2.2.2.3 Multicast

Se lo define como la comunicación de un host emisor a varios host receptores en una red. El formato es el mostrado por la **Figura 8-2**

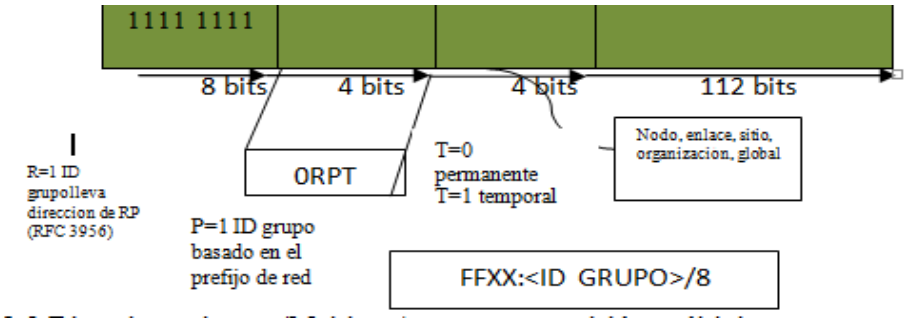


Figura 8-2 Direccionamiento (Multicast) para retransmisión múltiple
Fuente: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf)

IPv6dice que utilicen multicast, debido a que el protocolo inicial tiene mayores características en este tipo de direcciones. (DOS SANTOS R, MOREIRA A, ASSENCO REIS E, & SOARES DA ROCHA A, 2010, P.55-70)

Se da a conocer que los 8 primeros bits están en multicast puesto que están puestos en 1, los 4 bits que le siguen son banderas que indican si existen direcciones temporales. La **TABLA 8-2**muestra a cada uno de los bits de ámbito, que identifique el grupo, grupo multicast referido, de manera permanente o temporal.

Anycast toman direcciones del bloque FF00::/8, el prefijo FF es una multicast, representado por cuatro bits, que son llamados flags, y otro valor de cuatro bits que definen el alcance del grupo multicast. Los 112 bits identifican multicast . (DOS SANTOS R, MOREIRA A, ASSENCO REIS E, & SOARES DA ROCHA A, 2010, P.55-70)**VER igura9-2**

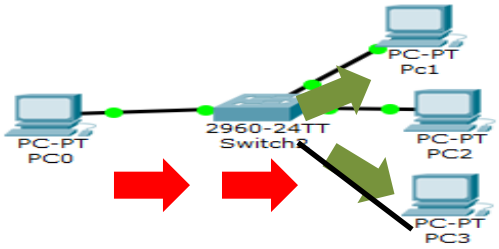


Figura 9-2 Direccionamiento Multicast
FUENTE: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf

En la **TABLA 8-2** explica para cada valor hexadecimal existe un direccionamiento multicas.

Tabla 8-2 Traducción de los bits de ámbito

Valor hexadecimal	Descripción
0	Reservado
1	Ámbito local de Nodo
2	Ámbito local de enlace
3	No asignado
4	No asignado
5	Ámbito local de sitio
6	No asignado
7	No asignado
8	Ámbito local de organización
9	Jumbogram
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ámbito global
F	Reservado

Fuente: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf)

En la TABLA 9-2muestra direcciones IPv6 y sus correspondientes direcciones multicast de nodo solicitado (COELLAR J & CEDEÑO J, 2013)

Tabla 9-2 Direcciones multicast de nodo

DIRECCIÓN IPV6 SOLICITADO	DIRECCIÓN MULTICAST DE NODO
2800:270:bcd0:3::1	Ff02::1:ff00:1
2800:270::1230:1000:a34:9e9a	Ff02::1.ff34:9e9a
2800:270::3de:2000:a34:9e9a	Ff02::1: ff34:9e9a
Fc00:0:0:1::aaaa:a1	Ff02::1::ffaa:a1

Fuente: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf)

2.2.3 *Caracteristicas de IPv6*

IPv6 es una mejora de IPv4, dentro de las mejoras se encuentra mayor direccionamiento, mayor velocidad, trabaja sin conexión y cuenta con una cantidad máxima de saltos, (LÓPEZ J, 2014, p. 18-25)

Mayor direccionamiento:

En IPv6 ocupa más bits que las versiones anteriores es decir 96 bits más que IPv4 con lo cual se obtienen 2^{12} direcciones aproximadas de red, permite múltiples divisiones de subred: **Ver Figura10-2**

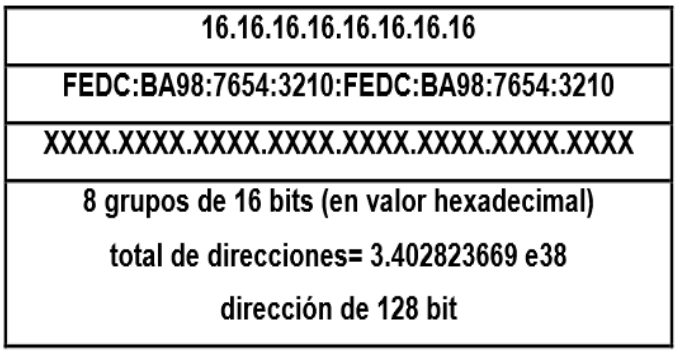


Figura 10-2 Representación de las direcciones IPv6
FUENTE: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf)

Si hay 0000 (ceros) se simplifica con un simple 0 ya que no es necesario escribir todos los ceros a la izquierda. Cuando 2 o más campos consecutivos están llenos de 0's (ceros) se puede simplificar de la siguiente manera: 0000:0000:0000: =:0:0:0:

Esta regla se usa cuando los campos con valor = 0 sean consecutivos y solo una vez se puede usar: en una dirección IP: por ejemplo:

2002:0450:0009:0010:0000:0000:0000:0071 = 2002:450:9:10::71

FFFF:0:0:0:FFFF:0:0:0 solamente se podrá comprimir en FFFF::FFFF:0:0:0 o en FFF:0:0:0:FFFF:: pero nunca EN FFFF::FFFF::

Si se encontrara así:: en una dirección, para conocer la dirección completa simplemente se llenan los campos faltantes con 0's hasta completar la dirección de 8 campos (VAZQUEZ AMENDARIZ W, 2005,p. 46)Ejemplos:**VER Figura 12-2**

FFFF::12	FFFF:0000:0000:0000:0000:0000:0000:0012
::5	0000:0000:0000:0000:0000:0000:0000:0005
1080::8:800:200C:417A	1080:0000:0000:0000:0008:0800:200C:417A
1::1	0001:0000:0000:0000:0000:0000:0000:0001

Figura 11-2 Representación numérica de las direcciones IPv6
FUENTE: (http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf

- **Rendimiento***:* Habla sobre la velocidad que tienen los datos. La evolución que tiene la tecnología ha mejorado el ancho de banda para obtener mayor rendimiento y velocidad de datos.(PINILLOS, 2003, p. 51-54)
- **Autoconfiguración***:* es más simple ya que se configura los 64 bits superiores son seteados por un mensaje desde el router y los 64 bits más bajos son seteados con la dirección MAC.
- **Simplificación del formato del Header**.- los campos del header IPv4 se quitan o se hacen opcionales.
- **Paquetes IP eficientes y extensibles**,- sin existir fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.
- **Posibilidad de paquetes con carga útil** (datos) de más de 65.355 bytes es decir millones de bytes útiles.
- **Seguridad** en el núcleo del protocolo (IPsec) .El soporte de IPsec es un requerimiento del protocolo IPv6, proporciona soporte nativo para seguridad basándose en sus cabeceras de extensión.
- Capacidad de etiquetas de flujo- .Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flor) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.
- **Remuneración y "multihoming":** facilitando el cambio de proveedor de servicios.
- **Características de movilidad**, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.

- **Ruteo más eficiente** *en el backbone de la red*, debido a la jerarquía de direccionamiento basada enaggregation.
- *Calidad de servicio* (QoS) y clase de servicio (CoS), Capacidades de autenticación y privacida (VAZQUEZ AMENDARIZ W, 2005,p. 48)
-

2.2.4 Fundamentos de ipv6

Los fundamentos de IPv6 se basan en el espacio mayor de direccionamiento ya que incrementa su tamaño de direcciones de forma volumétrica de 32 bits a 128 y así poder obtener un número mayor de nodos direccionables. Este diseño agrega múltiples beneficios en lo que seguridad se refiere así por ejemplo:

- Manejo de calidad de servicios
- Mayor capacidad de transmisión
- Facilidad de administración

IPv4 soporta 4, 294, 967,296 (2^{32}) direcciones que es poco menos que 4.3 billones, IPv6 ofrece $3.4x10^{38}$ (2^{128}) direcciones en números 6.67126144781401e+23 direcciones IP por cada metro cuadrado sobre a tierra. Adicionalmente, IPv6 fue diseñada para ser subdividida en dominios de enrutamiento.

2.2.5 Seguridad de redes

2.2.5.1 Antecedentes

En esta investigación que se está realizando está enfocado a realizar un framework para analizar riesgos e identificar las vulnerabilidades de seguridad que existen en el protocolo de IPv6 dentro de la red por donde viajan datos confidenciales de cualquier empresa, organización, entender y definir políticas, procedimientos y estándares de acuerdo a los requerimientos que la necesitan. Además existe software que ayudaran a atenuar los riesgos que se pueden presentar en la red.

Los conceptos de disponibilidad, confidencialidad, integridad son tres elementos fundamentales en la seguridad de la información para garantizar su autenticidad. Para garantizar esta seguridad se controla de dos maneras el físico y el lógico, tomando la configuración de algunos elementos hardware y software de seguridad como routers,

firewalls, IPS/IDS, Gateway etc.

Realizando este control de los dos elementos |garantiza el mejor desempeño y si existe algún problema (BUSTAMANTE SANCHEZ R, 2005, p. 2-10)

2.2.5.2 Tipos de seguridad en redes

Se clasifican en dos tipos, y de ellas se subdividen como se muestra en la **TABLA 10-2**y luego se definirán.

Tabla 10-2 Tipos de seguridad en redes de computadoras

1. SEGURIDAD FISICA	2. SEGURIDAD LOGICA
Desastres	Controles de acceso
Incendios	Identificación
Equipamiento	Roles
Inundaciones	Transacciones
Picos y ruidos electromagnéticos	Limitación a los servicios
Cableado	Control de acceso interno

FUENTE:(BUSTAMANTE SANCHEZ R, 2005, p. 2-10)

2.2.5.2.1Seguridad física

La seguridad física está orientada a brindar cuidado a los lugares, herramientas donde se encuentran los equipos de cómputo y por lo tanto se tiene la información confidencial, cuando un ladrón ingresa a las instalaciones donde se encuentran los datos es porque encontró vulnerabilidades físicas debido a que se le hace más fácil robar un CPU, discos duros, CDs, memory Flash, etc.

Si se nota através de medidas físicas que las instituciones están preocupadas por la seguridad probablemente abandonaran el ataque físico para lanzarlo en contra de otra red menos protegida(VILLALON HUERTA A, 2010,p. 20)La seguridad física se subdivide:

Desastres.-Son de origen natural y por el hombre entre ellos tenemos:

- Desastres naturales
- Desastres ocasionadas por el hombre.

- Disturbios, sabotajes internos y externos deliberados.

Según (BUSTAMANTE SANCHEZ R, 2005, p. 3)

Incendios.-son ocasionados por la naturaleza o por el hombre, cuando es natural hablamos de un rayo eléctrico y cuando es ocasionados por el hombre cuando no previene los peligros al realizar malas instalaciones eléctricas como sobrecargar una red, cortocircuitos por tener en mal estado el cableado y puede dar origen al incendio.
Cuando el incendio es de magnitudes mayores no se debe tomar en cuenta el manual de seguridad para salvar equipos ya que se debe salvaguardad a los usuarios, pero si es de menos proporción utilizar los extintores para salvar el equipo de cómputo, (VILLALON HUERTA A, 2010,p. 30).

Equipamient*o*.- el acceso a los equipos deben ser restringidos, deben contar con ventilación, detección de incendios y contar con la siguiente normativa:

- Su temperatura debe ser igual a 18° C
- Humedad no debe superar el 65% para evitar el deterioro
- Proveer los equipos contra incendios de acuerdo al departamento.
- Instalar extintores manuales

Esto expone (BUSTAMANTE SANCHEZ R, 2005, p. 6)

Picos y ruidos electromagneticos.- Para evitar los picos y ruido se deben tener las instalaciones eléctricas independientes que las de red de datos y cuando existen sobrecargas de electricidad que también ocasiona ruido deben contar con una toma a tierra.

Si los sistemas se complican tienen que estar el personal competente para analizar y corregir con normas de seguridad.(Rubén Bustamante Sánchez, 2005)

Cableado.- para que no existan daños en el cable es necesario normar en los edificios, domicilios, oficinas el cableado de redes de información para evitar tiempo y dinero.
Los inconvenientes que presenta el cable son: Interferencia, los cables de fibra óptica, corte del cable, Daños en el cable y Desviando o estableciendo una conexión no autorizada en la red (BUSTAMANTE SANCHEZ R, 2005, p. 7)

.

2.2.5.2.2 Seguridad lógica

Seguridad lógica trata decolocar barreras, paredes, procedimientos que resguarden nuestros sistemas informáticos, los hackers buscan los agujeros que no cubrieron estas barreras y mandan ataques de forma intencionada como software maliciosos, o simplemente por error bugs o agujeros (BUSTAMANTE SANCHEZ R, 2005, p. 7)

La seguridad lógica se sostiene en las técnicas siguientes:**VER TABLA 11-2**

Tabla 11-2 Técnicas de seguridad lógica

#	**TÉCNICAS DE SEGURIDAD LÓGICA**
1	Evitar el acceso a los programas y archivos.
2	Capacitar al personal que no pueden manipular programas ni archivos que no les pertenezcan.
3	Seguridad en el uso correcto de archivos y programas
4	Transmisión segura al destinatario.
5	Información integra.
6	Se integre sistemas alternativos de transmisión en diferentes puntos.
7	Se tenga planes alternativos en caso de emergencia.

FUENTE: (Antonio Villalón Huerta, 2002)

Controles de acceso

Este control se lo puede efectuar en el sistema Operativo, en los sistemas e aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario, para proteger de la utilización o manipulación de personas no autorizadas y mantener la integridad.

También determina si un permiso de acceso solicito un usuario a un recurso, el control de acceso conlleva dos procesos.
Identificación**.-E**s Cuando el usuario se da a conocer en el sistema
Autenticacióna la verificación que realiza el sistema sobre esta identificación. De acuerdo a («SEGURIDAD INFORMÁTICA», 2002)

Roles

Para tener acceso a los datos depende también de la funciones que desempeña el trabajador de la entidad para la cual labora como puede ser el gerente, director, el

analista En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios («SEGURIDAD INFORMÁTICA», 2002)

Transacciones

En este tipo de acceso se lo debe realizar a través de un mediador por medio de claves («SEGURIDAD INFORMÁTICA», 2002)

Limitación a los servicios

Estos controles limitan al personal que puedan utilizar las aplicaciones si autorización ya que cada una de las personas tienen funciones preestablecidas un mejor entendimiento seria cuando se contrata señal de tvcable para un solo equipo y si el usuario trata de repartir a otros equipos el control que tiene no le permitirá realizar esto ya que restringió el servicio(BUSTAMANTE SANCHEZ R, 2005, p. 7)

Control de acceso interno

Los controles de acceso interno cumplen con la función de proteger las entradas a ciertos directorios a través de cinco controles

- Palabras clave (password)
- Sincronización de passwords
- Caducidad y control
- Encriptación
- Listas de control de accesos
- Limites sobre la interfaz de usuario
- Etiquetas de seguridad

Control de acceso externo

Se refiere a la seguridad que se brinda a los siguientes elementos

- Control de puertos
- Firewalls
- Acceso de personal

- Acceso al publico

Encriptación

En este punto los datos originales se pueden obtener a través de una desencriptación por medio de las claves que posean las personas que tienen autorización, por medio de un control.

Listas de Control de Accesos

Esta lista de control tiene el personal que tiene permiso por medio de un registro que se lleva en el sistema.

Límites sobre la Interface de Usuario

Tienen los usuarios que cumplen funciones específicas para obtener la información donde se tienen registrados por medio de menús, base de datos e interfaces de usuarios.

Etiquetas de Seguridad.

Son denominaciones que se dan a los recursos. Estas etiquetas no son modificables («SEGURIDAD INFORMÁTICA», 2002)

2.2.6.3 *Políticas de seguridad*

La seguridad informática en los últimos tiempos ha tomado una verdadera importancia por la evolución de tecnológica disponible, el conectarse por medio de una red y enviar y recibir datos han abierto un sinnúmero de amenazas para obtener esta información.

Las amenazas que llevan consigo las informaciones importantes de una empresa pública o privada han abierto al personal que maneja las tecnologías de la información a desarrollar documentos, leyes para el uso correcto de los datos y obtener ventajas y no desventajas de las mismas. Con estas leyes limitan al personal que maneja la

información hacer uso indebido, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de las empresas(«SEGURIDAD INFORMÁTICA», 2002)
Las políticas de seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema.

Por la aparición de hacker y sus delitos se establecen políticas de seguridad en todas las instituciones para la mitigación de fallas y debilidades de sus software y entablar compromisos para mantenerse actualizados y modernizados en el tema de políticas al personal que labora en cada una de las instancias y evitar la fuga y el robo de información. («SEGURIDAD INFORMÁTICA», 2002).
En el ANEXO 2 se muestra las disposiciones generales emitidas sobre las políticas de seguridad informática.

2.3 Ataques y vulnerabilidades en el protocolo IPv6

2.3.1 *Conceptos de Ataque*.

Un ataque informático es una técnica que utilizan los hackers para obtener el control, desestabilizar o dañar un sistema informático por medio de otro sistema informático como son las PCS o la red, para disminuir estos ataques existen métodos para combatirlos y reducir esta acción.

Parar un ataque informático no depende solo de los software sino de la educación que se les brinde a las personas que ocupan un equipo de cómputo, que precauciones deben tomar en el momento que naveguen por la red que es el medio más común por donde los hacker aprovechan las vulnerabilidades y riesgos que están expuestos.
Los ataques tienen cinco fases por las suelen pasar se observa en la Figura **11-2**

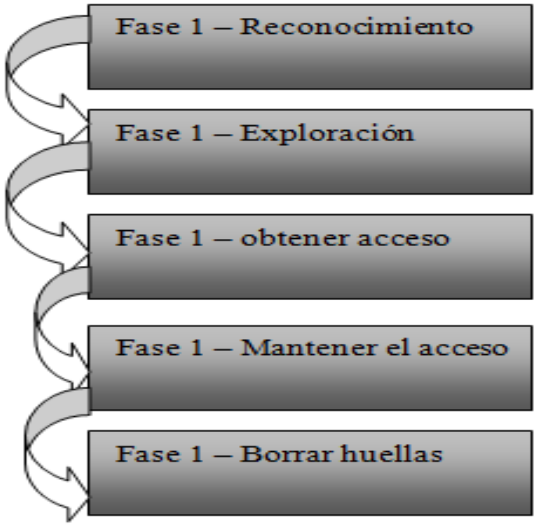


Figura 11-2 Fases comunes de un ataque informático
FUENTE:(JHOVANNY ZAPATA, 2010).

*Fase 1:*Reconocimiento.- es buscar información de la víctima a la cual quiere llegar utilizando métodos comunes como ingeniería social, programas informáticos a través de puertos de PC o cualquier medio que se pueda obtener información.
Fase 2: Exploración.- obtenida la fase 1 se procede a indagar y manipular los datos de la víctima de las cuales se puede obtener direccionamiento hosty otros datos que puedan ser de utilidad.

Las aplicaciones que un hacker utiliza para obtener estos datos son: network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

Fase 3: Obtener acceso.-para obtener acceso a los datos los intrusos utilizan técnicas como de explotación de vulnerabilidades obtenidas en las dos fases anteriores, estas técnicas son Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking.

Fase 4: Mantener el acceso.- cuando ya ingresan al sistema configuran el sistema para poder ingresar nuevamente sin dificultad para ello utilizan técnicas como backdoors, rootkits y troyanos.

Fase 5: Borrar huellas. – eliminar del sistema rastros que puedan ser descubiertos por los expertos, eliminara archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS), (MIERES J, 2009,p. 5)

2.3.2 ***Tipos de ataques a la red***.

Las redes frecuentemente están expuestas a los ataques por parte de hackers las cuales se dividen en ataques activos y pasivos.

*2.3.2.1 Ataques activos***:**

Son los que producen cambios en la información y en la situación de los recursos del sistema. En los ataques activos se subdividen en cuatro categorías: **Suplantación de identidad**, **Re actuación, Modificación de mensajes, y Degradación fraudulenta del servicio**(CASTAN SALINAS A, 2007,11-22)**VER Figura 12-2**

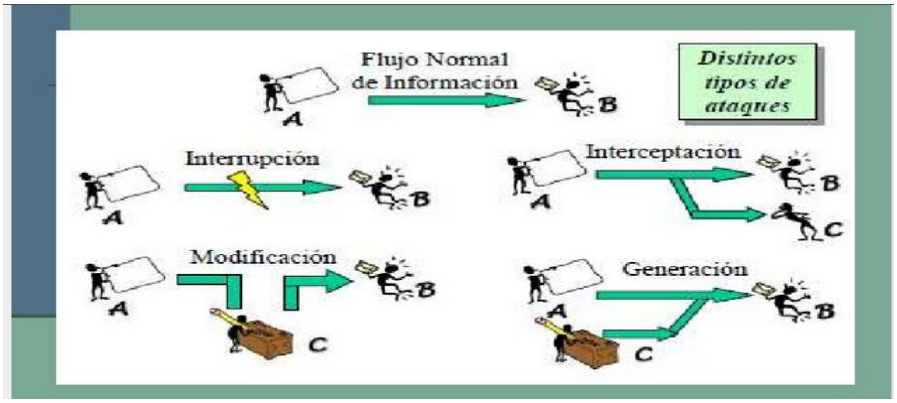


Figura12-2 Distintos tipos de ataques
Fuente:(UBENGA FERNÁNDEZJ, 2011)

En los protocolos IPv6 existen ciertos tipos de ataques que se pueden dar relevancia en la investigación que se realizara sobre la detección de errores en la infraestructura de IPv6 numeramos unas de ellas:

- Ataque por medio del envío de Paquetes de Router Advertising, y DHCPv6:
Éste tipo de ataque va dirigido a redes que son nuevas y no están preparadas ni implementadas en seguridad

Para este ataque se debe contar con una PC dentro de la red que simule un router que está su prefijo IPv6 por medio de paquetes de "Router Advertisement", y la victima configure por defecto el Gateway a la dirección IP versión 6 de la máquina atacante.

Se logra que la víctima salga a internet y se aun flanco fácil para revisar y cambiar datos con ello el atacante puede actuar como servidor DNSv6.

Ataque a través de "Extensions Header's" en paquetes "Discovery" y "Advertisement"

El uso de "Extension Header's" provee al atacante maneras de eludir los mecanismos de defensa que posee la red (RA-Guard RFC - 6105). Fernando Gontmanifiesta que ignore paquetes Discovery y Advertisement que contengan "Extension's Headers", para no ser flancos de ataques.

El mecanismo (RouterAdvertisementGuard) controla la falsificación de paquetes en un mecanismo de capa2 consiste en eliminar los paquetes RA de los puertos puesto que son fáciles para engañar el, por lo que si se tiene un "Extension Header" en el paquete, por allí se puede enviar la información que pertenece a un paquete RA y así engañar el filtrado de RA - Guard**VER Figura 13-2**

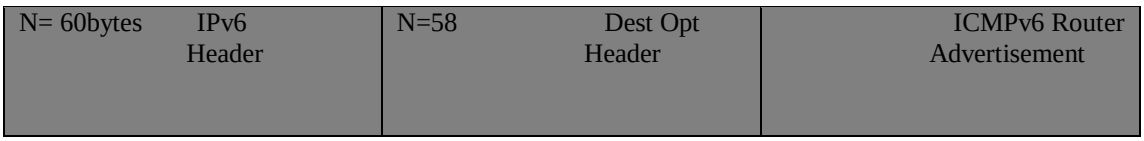


Figura 13-2 Extensión Header IPv6
Fuente:(sourcebook, 2011)

Ataque a través del uso de Fragmentación de Paquetes

Esteataque es una técnica donde el hacker genera e inyecta paquetes IPv6 encriptados a la red este tipo de ataque se centra en capturar el paquete encriptado, lo que hace es añadirle una cabecera de "Header Fragmentation" en la que se tiene como "Fragmentation Value " y el bit "M" con valores '0'; este tipo de paquetes pueden ser creados por medio del envío de paquetes ICMPv6 'Packet Too Big Error', con ello ya puedo utilizar éstos headers para causar ataques como DoS de un flujo de datos de una víctima específica(como se indica en 'draft-gont-6manpredictable-fragment-id') pues con los Fragment Header se puede hacer creer que los paquetes que envíe la victima son

todos resultado de una colisión y por lo tanto deben ser descartados; como este ataque también existen otros ataques que aprovechan las vulnerabilidades que tienen los paquetes que utilizan “Fragment’s Headers”.

Los fragmentos de un paquete IPv6 normal de datos, tal y como se muestra en la siguiente Figura 14-2(GARCIA MARTIN C, 2012,p. 33)

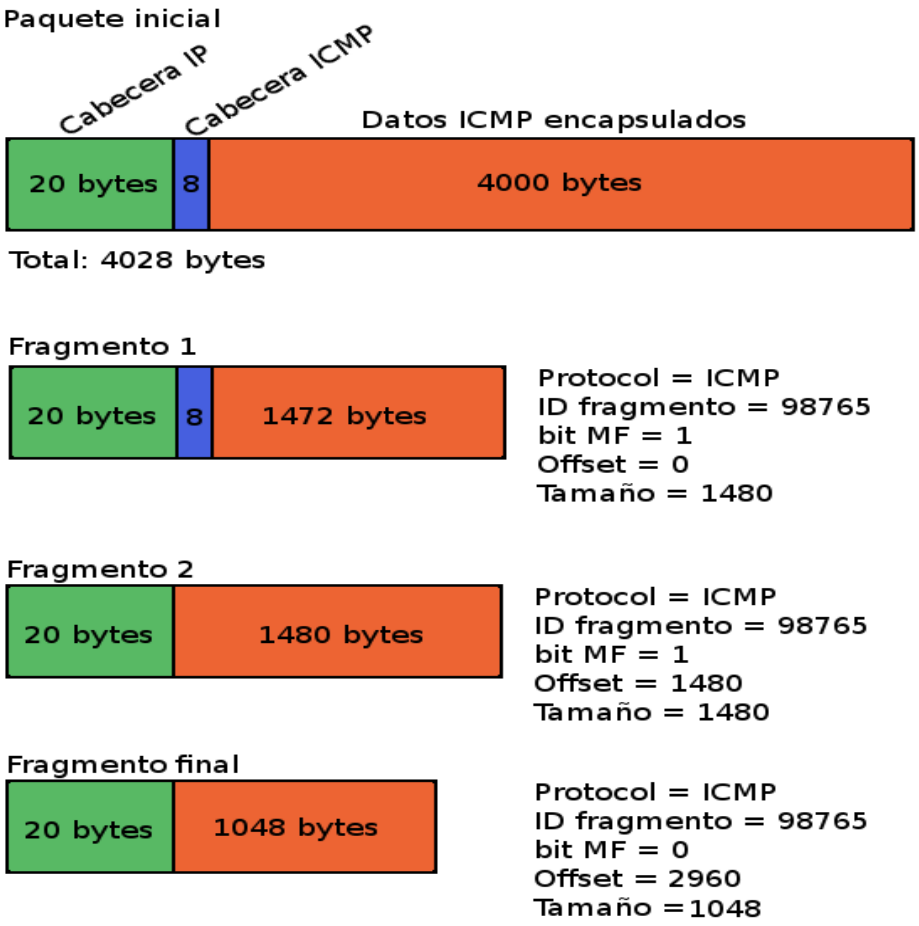


Figura 14-2 Uso de Fragmentación de Paquetes
Fuente: (CARRASCO P, 2010)

- *Ataques derivados de Cabeceras de Extensión*

La especificación del protocolo IPv6 indica un orden recomendado para las cabeceras de extensión y que ninguna (salvo alguna excepción) puede aparecer más de una vez en el paquete, mediante la utilización de técnicas de Packet Craftinges fácil crear paquetes que no sigan estas recomendaciones. Por ejemplo, podrían crearse paquetes con una larga lista de cabeceras de extensión con el objetivo de crear un ataque DoS (Denial of Service), producir un aumento en el uso de la CPU, recursos, etc. Además, si el

software no trata correctamente estos casos, el paquete puede producir un error del sistema o un comportamiento no deseado.

En los siguientes subapartados se comenta un poco más en detalle los riesgos que puede causar cada cabecera de extensión.

Cabecera Hop-By-Hop y Destination Options

Tanto la cabecera Hop-By-Hop como Destination Options deben aparecer una sola vez en el paquete, por lo que cada nodo debe comprobar que se cumple esta condición, sin embargo, no hay restricción en el número ni en el orden de las opciones que pueden aparecer en la cabecera., esto puede ser causa de problemas debido a que la inclusión de un gran número de opciones puede aumentar la carga de procesamiento del nodo
Sin embargo, si enviamos un paquete de este tipo con cierta información en el payload la víctima puede que no procese dicho payloady no detecte el error. Otro proceso en la máquina de la víctima puede estar atento a esta información y por tanto disponer así de un canal de comunicación encubierto.

Otra de las opciones que tiene implicaciones en la seguridad es la opción Router Alert, esta opción indica a los routers que deben analizar el contenido de la cabecera, un usuario malicioso podría enviar un gran número de paquetes haciendo que el consumo de recursos aumente significativamente.

La forma de mitigar estos ataques es incluir reglas en el ACL (Access Control List) de los routers con el objetivo de no procesar estas opciones y limitar este tipo de paquetes (GARCIA MARTIN C, 2012,p. 31)

1. Cabecera de Routing.

La cabecera de Routing contiene dos tipos válidos hasta el momento: tipo 0 (RH0) y tipo 2 (RH2), la cabecera RH0 ha quedado obsoleta por cuestiones de seguridad pero es conveniente revisar este caso como ejemplo de las implicaciones que puede tener una mala especificación del protocolo. Esta cabecera tiene una función similar a la que tenía la opción source routing en IPv4, puede utilizarse para reencaminar el tráfico a

través de uno o varios hosts intermedios, esta funcionalidad puede utilizarse con varios fines maliciosos.

El primero es el de dirigir el tráfico por ciertos caminos con el objetivo de atravesar equipos que no detectan este tipo de tráfico haciendo posible un ataque man-in-the-middle.

El segundo uso que un atacante puede dar a estas cabeceras nace del hecho de que la especificación no incluía ninguna prohibición acerca de las direcciones por las que se quiere reenviar el tráfico, de esta forma, podría utilizarse para amplificar la carga de tráfico incluyendo las mismas direcciones varias veces en la cabecera de Routing, provocando una denegación de servicio de la (GARCIA MARTIN C, 2012,p. 33)Este proceso se puede **ver Figura 15-2**

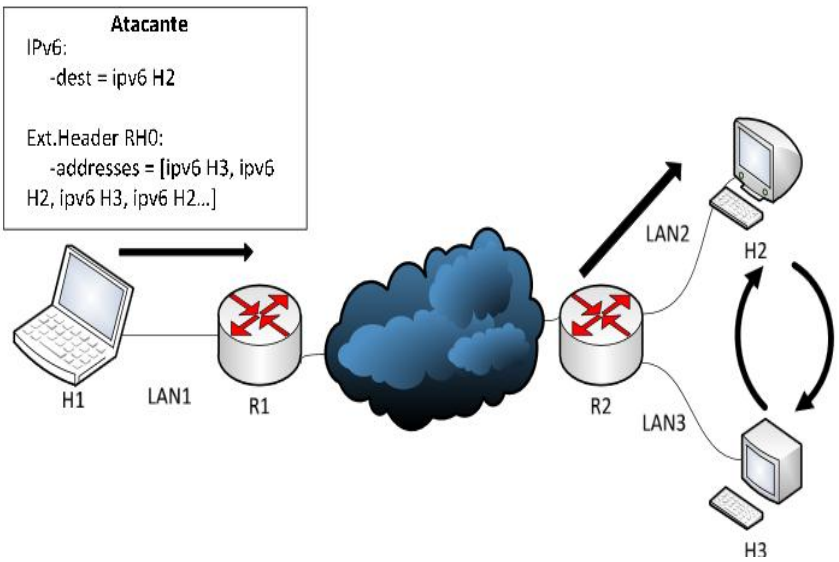


Figura 15-2 Ataque en la Cabecera de Routing
Fuente::(GARCIA MARTIN C, 2012,p. 33)

2. Cabecera Fragmentación.

La MTU mínima que se define en IPv6 es de 1280 bytes por lo que los paquetes de menor tamaño pueden ser sospechosos, sin embargo, existe un caso donde si se permite el uso de fragmentos de menor tamaño en IPv6: sies el final del paquete es donde el atacante oculta datos dañinos. De esta forma, la fragmentación puede utilizarse para ofuscar información que no se desea que sea analizada por el Firewall.

3. Ataques derivados de ICMPv6

Con IPv4 el protocolo ICMP no es esencial para la comunicación, pero en IPv6 los mecanismos de configuración más importantes se realizan a través de ICMPv6. Por este motivo el protocolo ICMPv6 es un objetivo clave para los atacantes, especialmente en entornos de red local.

Los ataques basados en este protocolo se pueden clasificar por el mecanismo que utilizan: SLAAC, Neighbor Discovery, detección de direcciones duplicadas y redirección.

4. Satateless Address Autoconfiguration (SLAAC)

El mecanismo hace que un host pueda configurarse de forma autónoma para comunicarse en una red, aunque esto ofrece grandes beneficios y es uno de las principales mejoras introducidas en IPv6, también conlleva importantes riesgos de seguridad que han derivado en la aparición de varios tipos de ataques.

Con este modo de funcionamiento, los routers anuncian su dirección mediante mensajes Router Advertisement (RA), así, el router manda periódicamente mensajes RA para que los host puedan configurarse su propia dirección y tabla de routinga partir de la información que transporta.

Dado que no se emplea ningún mecanismo de autenticación, un atacante podría capturar estos mensajes, inspeccionar la información y enviar él mismo los mensajes modificados indicando una dirección de capa de enlace falsa, esto causaría una denegación de servicio ya que el resto de hosts enviarían la información a una dirección falsa. En la **ILUSTRACIÓN 18** se puede ver el esquema de este ataque, dónde el atacante anuncia la dirección MAC falsa (XX:XX:XX:XX:XX:Xe)**ver Figura 16-2**

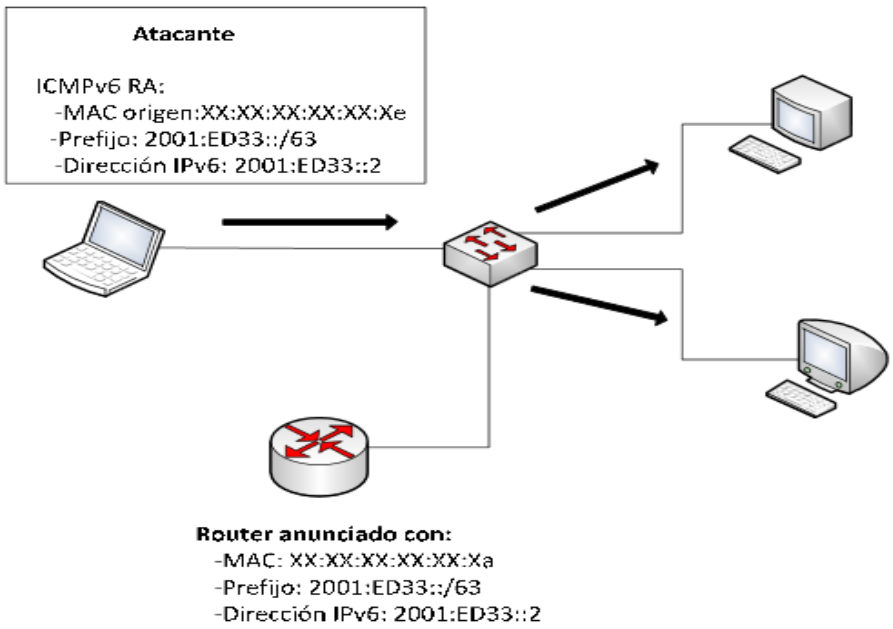


Figura 16-2 Ataques RA falso derivados de ICMPv6
FUENTE: (GARCIA MARTIN C, 2012, p. 72)

5.Neighbor Discovery

El protocolo ARP para descubrimiento de vecinos utilizado en IPv4 recae ahora en ICMPv6 a través de los mensajes Neighbor Advertisement (NA) y Neighbor Solicitation (NS), englobados en el protocolo Neighbor Discovery (NDP), como ocurría con SLAAC, NDP tampoco utiliza autenticación por lo que es fácil suplantar la identidad de otro usuario.

Un primer ataque sería similar al comentado sobre SLAAC, pero en este caso enviando mensajes NA con la dirección IPv6 de la víctima y una dirección de capa de enlace falsa. De esta forma se crea una denegación de servicio sobre la víctima dado que los mensajes se enviarán a una dirección de capa de enlace que no corresponde con la real.

En un segundo ataque sobre NDP, un usuario malicioso podría hacer spoofing de mensajes NA y NS. Si el atacante obtuviera la dirección MAC del router, podría suplantar su identidad haciendo un ataque MITM (Man in the Middle, Figura) a cualquier usuario de la red local. Mediante este procedimiento el atacante podría realizar cualquier acción sobre el tráfico de la víctima. **Ver Figura 17-2**

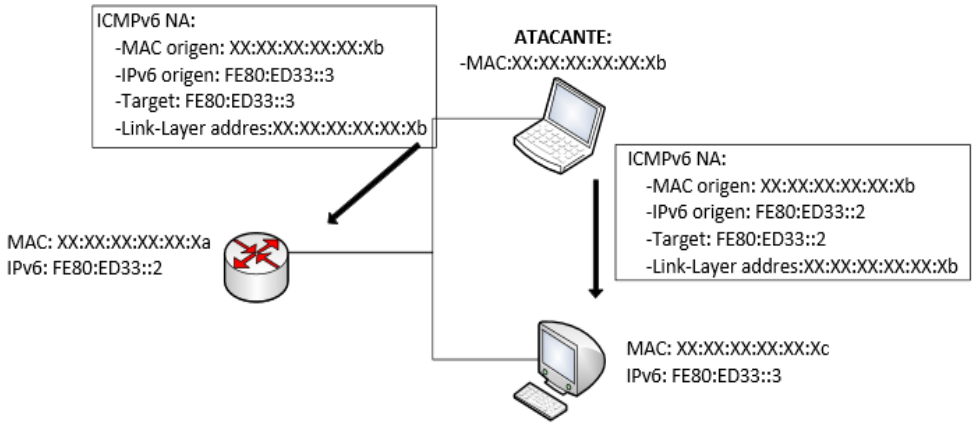


Figura 17-2 Ataque Neighbor Discovery man in the middle
Fuente: (GARCIA MARTIN C, 2012,p. 74)

Otro ataque que podría llevarse a cabo mediante NDP, trata de explotar el alto espacio de direccionamiento que soporta IPv6, una configuración de red típica permite tiene un prefijo de 64 bits, lo que nos da opción de configurar 264 direcciones IPv6, los routers deben contener una tabla actualizada con cada dirección configurada en la red, necesaria para reenviar el tráfico. Sin embargo, el tamaño de estas tablas no es suficiente para almacenar todo el rango de direcciones, lo que permite a un atacante enviar un flooding de mensajes NA con direcciones aleatorias de forma que se llene la tabla NDP, así, ningún usuario un solo host ocuparía todos los recursos, denegando el acceso a la red a nuevos usuarios (DoS) ; el comportamiento de los equipos ante esta situación anómala puede ser inesperado, pudiendo afectar a otras interfaces de red (GARCIA MARTIN C, 2012,p. 74)

6. Detección de direcciones duplicadas

El mecanismo DAD (Duplicate Address Detection) forma parte del protocolo SLAAC y permite que los hosts comprueben si una dirección IPv6 auto configurada está siendo utilizada por otro host, mediante mensajes NS, de nuevo no se utiliza autenticación y un atacante podría modificar estos mensajes para crear una denegación de servicio sobre un usuario. Simplemente tendría que responder a los mensajes NS utilizados en el mecanismos DAD, indicando que la dirección está ocupada, si esto se hace para todos los mensajes, el host no podría configurarse nunca una dirección IPv6.

7. Redirect.

La redirección en IPv6 permite a un router indicara un host de que existe una mejor ruta hacia otro host ,el proceso es como sigue: un host HA tiene configurada una ruta por defecto hacia el router R2y en la red existe el otro router R1, en algún momento R2 detecta que existe una mejor ruta de salida para HA que pasa por R1, cuando HA necesita enviar un paquete, lo hace por R2 y este le informa de que la ahora la mejor ruta es a través de R1 mediante un mensaje ICMPv6 redirect. HA cambia su tabla de rutas.

En este caso si existe un mecanismo de protección: una copia del mensaje que causa la redirección se debe incluir en el mensaje ICMPv6 redirect, de esta forma se evita que un atacante envíe mensajes falsos. Sin embargo, esta restricción se puede bordear fácilmente, si el atacante envía un Ping a la víctima, éste sabe que la respuesta va a ser un mensaje ICMPv6 Echo Reply por lo tanto, al atacante le basta con incluir este mensaje en el mensaje ICMPv6 Redirect para falsearlo(GARCIA MARTIN C, 2012,p. 76)

8. Secure Neighbor Discovery (SEND)

Como acabamos de ver el protocolo NDP aparte de tener un destacado papel en IPv6, supone una gran superficie de ataque, siendo vulnerable a varios ataques. Es por esto que se han definido una serie de especificaciones que proporcionan mecanismos de seguridad al protocolo NDP (GARCIA MARTIN C, 2012,p. 77)

2.3.2.2 Ataques pasivos:

Lo que hace es solo tener información pero no la toca para ser manipulada, lo único objetivo es mantenerse informado de lo que sucede con ella***, la***técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtener el origen y destinatario de la comunicación
- Controlar el volumen de tráfico
- Controlar las horas habituales de intercambio de datos.

Los ataques pasivos no son detectados con facilidad Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante (CASTAN SALINAS A, 2007,19)

2.3.3 Conceptualización de vulnerabilidades

Son debilidades que muestran los sistemas informáticos al no contar con la seguridad requerida los atacantes buscan los mecanismos para debilitar la seguridad y explotar la confidencialidad, integridad y disponibilidad de la información.
Los hackers tienen muchos propósitos al ejecutar un ataque como el de demostrarse a ellos mismo el reto y sacar provecho económico.

Los ataques son causados por dos clases de fuentes:

1. Usuarios autentificados, son las personas que no tienen acceso directo a los sistemas informáticos es decir a parte de la red, estos pueden ser empleados internos que tienen conocimiento de seguridad o colaboradores externos con acceso a sistemas dentro de la red de la empresa que se les llama insiders. Y desde ese punto ya se registra vulnerabilidades.

2. Atacantes externos a la ubicación física de la empresa, accediendo por mecanismos remotosy se los llama outsiders. Un ejemplo de ataque podría ser la realización del análisis de un sistema, mediante fingerprinting, tras el cual es posible explotar una vulnerabilidad como un buffer-overflow de un servicio TCP/IP, enviando paquetes que parecen válidos mediante IP spoofing. Dentro de los métodos no se han incluido ataques de alto nivel, como por ejemplo la distribución y ejecución de virus a través del correo electrónico (protocolo SMTP), ya que afectan a vulnerabilidades particulares de las aplicaciones y los lenguajes de programación soportados por éstas. (SILES PELAEZ R, 2002,P. 25-40)

2.3.4 Tipos de vulnerabilidades de red

Las vulnerabilidades se dividen de acuerdo a los siguientes criterios:
- Número de paquetes expuestos en el ataque:

- Atomic: se requiere un único paquete para llevarla a cabo.
- Composite: son necesarios múltiples paquetes.

- Información necesaria sobre las cabeceras y los campos del protocolo que se usa para llevar a cabo el ataque:

- Context: se requiere únicamente información de la cabecera del protocolo.
- Content: es necesario también el campo de datos o payload (SILES PELAEZ R, 2002,P. 26)**ver tabla 12-2**

- **Tabla 12-2** Clasificación de Vulnerabilidades de acuerdo a criterios

Context	Ping of death Land attack winNuke	Port scan SYN Flood TCP hijacking
Content	DNS attack Proxied RPC IIS attack	SMTP attacks String matches Sniffing
	Atomic	**Composite**

Fuente (SILES PELAEZ R, 2002,P. 26)

En el protocolo IPv6 se presenta vulnerabilidad en el control Message Protocol versión 6 0 ICMPv6 y en las cabeceras de extensión. Los firewall y dispositivos de capa 3 deben descartar los paquetes que contienen las cabeceras de extensión que no son reconocidos, el problema es que algunos firewalls y otros dispositivos de red simplemente ignoran cualquier cabecera de extensión que no entienden entonces estos dispositivos pasan estos paquetes sin saber que esto podría ser parte de un paquete malicioso o un paquete manipulado. Doble pila, en IPv6 la vulnerabilidad puede heredarse de versiones anteriores es decir que si tenemos un servidor web puede estar abierto el puerto TCP tanto en IPv4 como en IPv6, si el filtrado se lo hace en IPv4 y no en IPv6.

Vulnerabilidades del DNS. IPv6 se basa más en DNS puesto que las direcciones más grandes son difíciles para recordar, el DNS contiene información sobre todos los sistemas IPv6 de la organización, por lo tanto puede ser utilizado para algunas actividades de reconocimiento, los atacantes pueden saber sobre la información almacenada en los servidores DNS para proceder con la recopilación de datos y generar los ataques posteriores (SILES PELAEZ R, 2002, 46-60)

2.4 Metodología OSSTMM

2.4.1 Introducción

La metodología OSSTMM es un manual que detalla un método adaptable a las pruebas de la seguridad, para esta investigación se utilizara los puntos que se requieran y se mostrara de forma sintética para dar a las personas que lean este documental un panorama general de los procesos en el análisis y pruebas de la seguridad. OSTMM fue creada para que se cumplan las reglas que establecieron organismos internacionales y hoy en día adoptaron los organismos nacionales como políticas que se deben cumplir en el entorno de la seguridad informática.

Las pautas que se van a seguir tienen que ir en conformidad y coordinación con la organización que va ser supervisada y que tomen esta metodología para realizar las pruebas de seguridad correspondientes.

OSSTMM vela por el cumplimiento de los parámetros preestablecidos en NIST, ISO 27001-27002 e ITIL entre otras. Se podría decir que es el manual más completo en lo que refiere a seguridad de la información(SAENZ GONZALEZ G, 2009, P.34)**Ver Figura18-2**

Figura 18-2 Logo de la Metodología OSSTMM
Fuente: (Pete Herzog, 2003)

2.4.2 Propósito de la metodología OSSTMM

ISECOM hace conocer el propósito que tiene esta metodología que fue probado científicamente para inspeccionar la estructura, realizando pruebas sobre la seguridad de adentro hacia afuera de un organización pública o privada.

Otro propio que dio a conocer el Instituto de seguridad es que esta metodología está abierta para entregar certificaciones a auditores de sistemas, este provee especificaciones para realizar los test de seguridad, la operacionalidad de los canales físicos, humanos, telecomunicaciones, vías inalámbricas, redes de datos.

Las recomendaciones de OSSTMM a seguir se toman las siguientes:

1. Las pruebas realizadas se la lleve a cabo a fondo
2. Incluir todos los canales que hagan falta
3. Las pruebas que se ejecuten cumplan con la ley
4. Se deben cuantificar los resultados
5. Verificar si los resultados son conscientes y repetibles
6. Los resultados tengan hechos como se deriva de las propias pruebas.

En esta investigación al utilizar el manual OSSTMM puede actuar como pauta para realizar pruebas de seguridad en La Escuela Superior Politécnica de Chimborazo, (HERZOG PETE, 2003,p. 46)

2.4.3 Tipos de test

Como se habló en el propósito la metodología OSSTMM realiza tipos de test para la verificación de la seguridad y se los ha divido en seis test como se lo numera a continuación **Ver Figura 19-2**

:• Test de Blindaje o Hacking Ético.
- Test de Doble blindaje, auditoría de Caja Negra o Pruebas de Penetración.
- Test de Caja Gris.
- Test de Doble Caja Gris.
- Test Tándem o Secuencial.
- Test Inverso

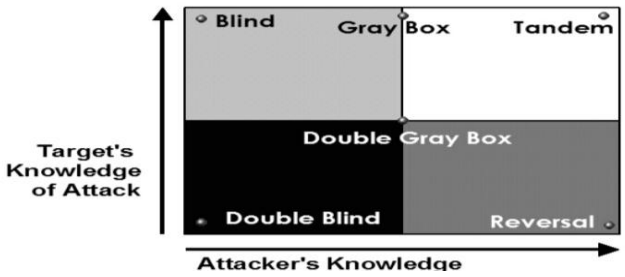


Figura 19-2 Tipos de test de OSSTMM
Fuente:,(HERZOG PETE, 2003,p. 13)

Blindado*:* El test Blindado no parte de una percepción es decir sin conocimientos previos de su defensa, El objetivo viene ya preparado listo para su auditoría conociendo todos los detalles de la misma. En este tipo es lo que se conoce también como "Hacking Ético" ,(HERZOG PETE, 2003,p. 13-16)

":

Este tipo de test no realiza ninguna notificación de la auditoria de las pruebas que se lo realizan, es una auditoria de penetración es decir consiste en pruebas ofensivas al mecanismo desde lo físico hasta el humano utilizando ingeniería social.

,(HERZOG PETE, 2003,p. 13-16)

De caja gris: Consiste en adquirir conocimientos básicos sobre defensa de ataques, el objetivo principal es saber los avances y sus detalles ,(HERZOG PETE, 2003,p. 13-16)

Doble caja gris*:* Tomando como primera parte en lo que consiste la caja gris a este test se amplia que es notificado el ámbito y el tiempo de cada marco de auditoria pero las pruebas no,(HERZOG PETE, 2003,p. 13-16)

Tándem o Secuencial (Tandem)*:* En este punto las dos partes el auditor y el objetivo conocen los detalles y se implanta las pruebas de protección y controles, en una prueba minuciosa.

Este es un proceso transparente por lo que se le llama de Caja de37 Cristal en el cual tanto el auditor como el objetivo trabajan en las pruebas ,(HERZOG PETE, 2003,p. 13-16)

Inverso: Se interactúa en el proceso y no se conoce **¿**Qué?, ¿Cómo? Y ¿Cuándo? la persona encargada de la auditoria se realizará las pruebas.

La meta es desconocida en este tipo de pruebas. La amplitud y profundidad depende de la calidad de la información provista al auditor. Esto permite por lo regular lo que se llama un Ejercicio de Equipo Rojo ,(HERZOG PETE, 2003,p. 13-16)

2.4.4 .Ámbito o competencia

OSSTMM tiene definido el ámbito que se debe abarcar en toda la seguridad operativa, es así que se observa en la siguiente **TABLA 13-2**

Tabla 13-2 Ámbito de competencia de OSSTMM)

CANAL	SECCION	DESCRIPCION
Seguridad Física	Humano	Todo el elemento humano comprometido en la organización
	Físico	Todo lo referente a las instalaciones y cualquier objeto tangible en la organización
Seguridad de las comunicaciones	Redes de Datos	Incluye todos los sistemas electrónicos y redes de datos que interactúan en la organización
	Telecomunicaciones	Son todas las comunicaciones digitales o analógicas empleadas para la comunicación entre redes
Seguridad del espectro electromagnético	Comunicaciones inalámbricas	Se incluyen todas las señales electromagnéticas empleadas tanto en las comunicaciones como en cualquier otro emanación del espectro

Fuente: (Aldo Valdez Alvarado, 2013)

2.4.5 Módulos

OSSTMM está dado por normas, regulaciones reglas, legislación y políticas definidas por esta metodología que como punto final se realiza comparación de todas las alarmas, alertas, reportes o registros de accesos esta metodología propone un modelo jerárquico de "CANALES, MÓDULOS Y TAREAS"

Los Módulos son áreas específicas de cada canal, pudiendo encontrar actividades que se encuentren en la frontera entre dos canales, la metodología lo que hace es dividir el trabajo de la auditoría clasificándolos por canales, módulos y tareas(VALDEZ ALVARADO A, 2013,p.1).

2.4.6 Fases de la metodología osstmm

La metodología de OSSTMM está conformada por cuatro fases, las cuales son las siguientes:

A. Fase de Inducción.

B. Fase de Interacción.

C. Fase de Investigación.

D. Fase de Intervención.

En la siguiente **TABLA 14-2**, es mostrado los módulos que constituyen cada una de las fases de la metodología, así como su descripción:

Tabla 14-2 Fases y módulos de la metodología OSSTMM

FASES	MODULO	DESCRIPCIÓN
Fase de introducción	Revisión de postura Logística	La revisión de reglas leyes, políticas aplicables al objetivo. Se define el alcance y las pruebas que deben hacerse, para realizar de manera correcta en la fase C La medición de los limitantes de interacción tales como distancia, velocidad y la fiabilidad de los resultados exactos
Fase de interacción	Verificación de la Detección activa Auditoria de la visibilidad Verificación de accesos Verificación de confianza Verificación de los controles Verificación de los procesos	La verificación de la práctica y de la amplitud de detección de interacción y la posibilidad de respuesta , para conocer restricciones impuestas a las pruebas interactivas y llevar adecuadamente las fases B y D Determinación de los objetivos que van a ser probados dentro del ámbito La visibilidad es considerada como presencia y no se limita a la vista humana La medición de la amplitud y profundidad de los puntos de acceso interactivos dentro del objetivo Determina relaciones de confianza de y entre los objetos. Una relación de confianza donde quiera que el objetivo acepte la interacción en el ámbito de aplicaciones Medición de utilización y eficacia de los controles de pérdida basados en procesos: el no repudio, Confidencialidad, privacidad e integridad. El control verifica al final de la metodología. Determinación de la existencia y eficacia del registro y mantenimiento de los actuales niveles de seguridad se definen por la revisión y postura los controles de indemnización La mayoría de los procesos tienen definidos un conjunto de reglas, sin embargo las operaciones no reflejan la eficiencia por lo que es necesario redefinir las reglas
Fase de investigación	Verificación de configuración Validación de propiedad Revisión de la segregación Verificación de la exposición Exploración de la inteligencia	La investigación del estado estable (funcionamiento normal) de los objetivos tal como han sido diseñados para funcionar en condiciones normales para determinar problemas de fondo fuera de la aplicación de pruebas de stress de seguridad La medición de la amplitud y profundidad en el uso de la propiedad intelectual ilegales o sin licencia o aplicaciones dentro del objetivo Determina los niveles de identificación de la información personal definido por la revisión de la postura. Sabemos cuáles son los derechos de privacidad que se apliquen y en qué medida de la información detectada como personal puede ser clasificada. Es la búsqueda de información libremente disponible que describe la visibilidad indirecta de los objetivos o los activos en el canal elegido por el alcance La búsqueda de información libremente disponible directa o

	Competitiva	indirectamente, que podría perjudicar o afectar negativamente al propietario del objeto a través de medios externos. Descubrir información que por sí solo o en conjunto pueden influir en las decisiones de negocios
Fase de intervención	Verificación de la cuarentena Auditoria de privilegios Validación de la supervivencia /continuidad del servicio Revisión de alertas y registros/ estudio Final	Determinación y medición del uso eficaz de la cuarentena para todos los accesos hacia y dentro del objetivo. Determinar efectividad de los controles de autenticación y el sometimiento en términos de cuarentena y listas blancas y negras El mapeo y la medición del impacto del mal uso de los controles de sometimiento, las credenciales y los privilegios o la escalada no autorizada de privilegios. Para garantizar la eficacia en los controles de autenticación deben ser registrados a profundidad. Calcular el número de denegación de servicios que se efectúa y su capacidad de recuperación Se realiza una auditoria a las tareas realizadas y se observa si se cumplió con el registro de actividades que tienen que cumplir Se pretende saber que partes de la auditoria dejo un rastro útil confiable

Fuente: (http://es.scribd.com/doc/210869601/OSSTMM-es-2-1)

Representacion en bloques de la metodologia OSSTMM

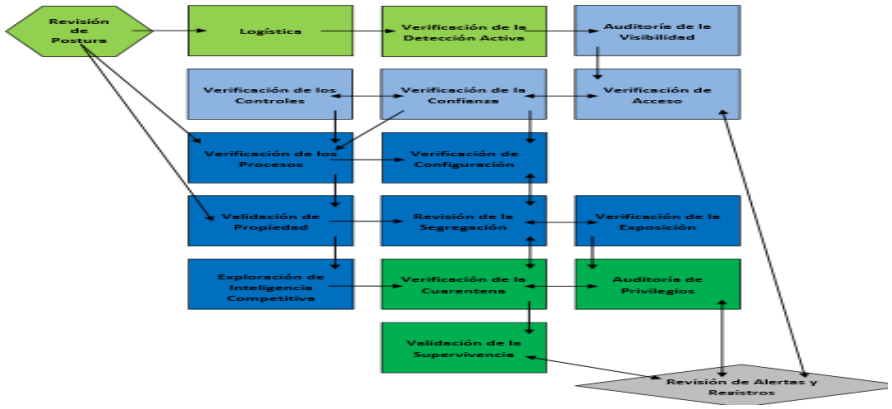


Figura 20-2 Representación en Bloques de la Metodología OSSTMM
Fuente: (http://es.scribd.com/doc/210869601/OSSTMM-es-2-1)

La metodologia OSSTMM son procdimientos que ayuda a seguir pasos ordenados para mantener intacta la informacion del antes , durante y despues que se realiza la prueba de seguriadad, esta metodologia dividido en secciones para obtener resultados en cada uno de los ambitos informaticas , según ISECOM instituto de seguridad tenemos la TABLA 15-2 que divide a la metodología en secciones:

Tabla 15-2 Secciones de la metodología OSSTMM

Seccion	Ambito de la seccion	Descripcion de ambitos
A	**Seguridad de la Información**	Evaluación de la Inteligencia, Privacidad y Recolección de Documentos
B	**Seguridad de los Procesos**	Controlar la Solicitud, Sugerencia Dirigida y Personas Confiables

C	**Seguridad en las tecnologías de Internet**	1. Logística y Controles 2. Sondeo de Red 3. Identificación de los Servicios de Sistemas 4. Búsqueda de Información Competitiva 5. Revisión de Privacidad 6. Obtención de Documentos 7. Búsqueda y Verificación de Vulnerabilidades 8. Testeo de Aplicaciones de Internet 9. Enrutamiento 10. Testeo de Sistemas Confiados 11. Testeo de Control de Acceso 12. Testeo de Sistema de Detección de Intrusos 13. Testeo de Medidas de Contingencia 14. Descifrado de Contraseña 15. Testeo de Denegación de Servicios 16. Evaluación de Políticas de Seguridad
D	**Seguridad en las Comunicaciones**	Control de PBX, Correo de Voz, FAX y Modem
E	**Seguridad Inalámbrica**	Comprobación de Radiación Electromagnética (EMR), de Redes Inalámbricas [802.11], Redes Bluetooth, Dispositivos de Entrada Inalámbricos, Dispositivos de Mano Inalámbricos, Comunicaciones sin Cable, Dispositivos de Vigilancia Inalámbricos, Dispositivos de Transacción Inalámbrico, RFID, Sistemas Infrarrojo y Revisión de Privacidad
F	**Seguridad Física**	Observación del Perímetro, monitoreo, Controles de Acceso, Respuesta de Alarmas, Ubicación y del Entorno

Fuente: (http://es.scribd.com/doc/210869601/OSSTMM-es-2-1

Esta investigacion se centra en la seguridad de los protocolos IPv6 con analisis exsausivos y minusiosos, quiere decir que se tomara como base la seccion C ya que esta seccion trata exclusivamente de la seguridad de las tecnologias del internet y profundisa sobre los protocolos.

Como se conoce el manual abarca modulos fases y secciones aquí se centrara en la seccion c.

SECCION C. Seguridad en las tecnologías de Internet metodologia OSTMM

En esta seccion se divide en 16 puntos de seguridad que hay que tomar en cuenta en el momento de asegurar las tecnologias de internet, se detalla a continuacion cada uno de los puntos de seguridad:

1. Logística y Controles

Aquí son detectados los llamados falsos positivos y negativos y se comprueban los Errores, se numera los paquetes medidos y examinados:

a) Examina la ruta y busca los paquetes perdidos TCP, UDP, ICMP.

b) Mide el tiempo de recorrido TCP de los paquetes y la latencia TCP a través de conexiones TCP.

c) Mide el porcentaje de paquetes aceptados y respondidos por la red objetivo y la cantidad de paquetes perdidos o rechazos de conexión en la red objetivo.

d) Examina el camino de enrutamiento al objetivo desde los sistemas de ataque, el camino de enrutamiento para el ISP del objetivo, el camino de enrutamiento para el Vendedor de Trafico Principal del ISP objetivo y el uso de IPv6 para cada uno de los sistemas activos en la red.

Estos puntos que son analizados se los toma del documento OSSTMM, (HERZOG PETE, 2003,p. 49)

2exploración o sondeo de Red

La sección de sondeo de datos trata de la obtención de información y la recopilación de datos de los sistemas de información a analizar, se puede decir que es lo más recomendable hacer para encontrar los puntos débiles que le aquejan a un sistema informático, es recomendable buscar los nombres de sistemas o IPs, lo recomendable en la metodología y políticas legales es buscar el número de sistemas que van a ser analizados, lo cual sería la inicialización de este test, en este punto se busca los rangos de direcciones a probar aquí no se realiza intrusión directa, (HERZOG PETE, 2003,p. 50)

3. Respuestas del Servidor de Nombres.

a) Analizar datos del dominio para buscar servidores y ver el dueño del bloque de direcciones IP.

b) Preguntar sobre los servidores y encontrar los hosts, subdominios, bloques IPs IPv6 por medio del DNS.

- Examinar la pared externa de la red y pistas de la organización a analizar.

a) Reconocer eventos de sistemas y filtración de información

b) Sondear código fuente, cabeceras de correos electrónicos, información sobre grupos de noticias

c) Buscar en bases de datos, servicios P2P conexiones dentro de la red objetivo y datos referentes a la organización.

Tomado del manual OSSTMM , (HERZOG PETE, 2003,p. 51)

4. Identificación de los Servicios del Sistema

Se caracteriza con la identificación de puertos,protocolos tunelizados, encapsulamiento y los servicios de internet y dará como resultado la existencia de agujeros que puedan traspasar a los cortafuegos. Las prueba en los diferentes protocolos dependerá del tipo de sistema y servicios que ofrecen los sistemas estimando un listado de protocolos en lo que se refiere al protocolo IPv6 en TCP y UDP en donde siempre se incluye el puerto 0, el testeo se lo deje a libre decisión del equipo, OSSTMM , (HERZOG PETE, 2003,p. 52)y se lo detalla a continuación :

5. Enumeración de sistemas

1) Que recolecta el broadcast desde la red, intenta sobrepasar los cortafuegos, determina la existencia de todos los sistemas en la red, emplea paquetes TCP con puerto origen 80 para todos los sistemas de la red; utiliza paquetes TCP fragmentados directos e indirectos y escaneos TCP SYN, conexione a DNS, SYN TCP, TCP full para todos los servidores de la red.

También usa FTP y Proxies para todos los servidores de la red enumeración de Puertos, escaneos UDP para enumerar puertos abiertos o cerrados para los puertos UDP por defecto.
Verificar y examinar el uso de tráfico y protocolos de enrutamiento, protocolos no estándar, protocolos cifrados, TCP e ICMP y respuestas a nivel de ´paquete.

2) Identificar la predictibilidad de los números de secuencia TCP, TCP ISN, generación de secuencia IPID, up-time del sistema, Servicios, Relacionar cada puerto abierto con un servicio y protocolo.
3) Reconocimiento de parchado del sistema, versiones, remapeo, componentes, usar peticiones de troyanos, ver el tipo de sistema operativo y de sus aplicaciones
4) Verificación y búsqueda de secuencias TCP para todos los servidores de la red, ofertas de trabajo boletines técnicos y ajuste de resultados, , (HERZOG PETE, 2003,p. 53)
5) Búsqueda de Información Competitiva
En la búsqueda de información útil a partir de la presencia que se tiene en Internet y que puede ser tratada como información sobre el negocio(HERZOG PETE, 2003,54)

6. Información del Negocio

Estructura mide examina y determina la estructura de directorio de los servidores web del FTP, WHOIS, SO, aplicaciones oferta de trabajo, cantidad de personal, entusiasmo, socios.

Registra.- identificanúmero de productos que se venden, número de productos encontrados en fuentes P2P, sitios de software pirata, cracks disponibles para versiones específicas y documentación tanto interna como de terceras partes sobre los productos.
Verifica la compra de productos, devoluciones contratos realizados por medio del internet.

Revisión de Privacidad.-Verificación que solo la persona que está encargada conoce lo datos y no el público, aquí se manifiesta la ética y moral del empleado
Como en todas las sesiones de este manual tenemos que seguir los pasos que recomiendan ya que estamos utilizando esta , (HERZOG PETE, 2003,p. 55)

Política.-Se toma en cuenta que el personal Identifica la política de privacidad pública, formularios web, base de datos, datos recolectados por la organización, localización de datos almacenados, tipos de cookies su expiración los métodos cifrados.

Identifica laclaridad y facilidad de la información con opt-out, gifs de publicación, bugs, personas, instituciones de forma positiva y negativa

7. Obtención de Documento*s*

Como primer punto se confirma la información por su cuantía dependiendo siempre del tamaño de la empresa, para un auditor no es nada el tiempo y la cantidad de información si no el tipo de información que puede obtener ya que le puede dar pautas para conseguir más datos confidencial. Hay que regirse a los pasos que recomienda el manual sin omitir alguno que son tomados de , (HERZOG PETE, 2003,p. 56)

Se exploran bases de datos web se indaga a los individuos claves se extrae todos los correos de e-mail se buscan noticias, documentos que tengan confidencialidad y examina redes peer-to-peer

8. Búsqueda y Verificación de Vulnerabilidades

Para la búsqueda de vulnerabilidades hoy en día es de gran ayuda los software, ya que son eficaces tanto en tiempo como en dinero este test identifica brechas de seguridad, es importante para los auditores identificar e incorporar en las pruebas que realizan los scripts y exploits que existen. No obstante, es necesaria la verificación manual para eliminar falsos positivos, La búsqueda manualizan la creatividad, la experiencia y la ingenuidad para probar la red objetivo , (HERZOG PETE, 2003,p. 57)

9. Testeo de Aplicaciones de Internet

Son pruebas en las aplicaciones, software para buscar fallos de seguridad como cliente/servidor de un sistema desde Internet, como ejemplo existen Aplicaciones web para transacciones entre empresas es un objetivo en este módulo. Test como "Caja Negra" y/o "Caja Blanca" pueden ser utilizados en este módulo, (HERZOG PETE, 2003,p. 58)

10. enrutamiento

Registra flujo de tráfico entre redes trabaja con políticas de seguridad utilizando ACL's puesto que acepta o deniega paquetes, este test asegura lo necesario lo demás lo desecha. La seguridad restringe el flujo de tráfico, lo routers cambian cada día que cuentan característica, el papel del auditor es en parte determinar la función del router dentro de la DMZ, (HERZOG PETE, 2003,p. 59)

11. Testeo de Sistemas Confiados

En este tipo de testeo se centra en los sistemas de confiados utilizando los siguientes pasos: Confirma el Testo de Aplicaciones y Servicios, sistemas y aplicaciones que puedan ser engañados además las prueba relacionada con eventos de engaño de origen.

12. Testeo de Control de Acceso.

Este módulo está diseñado para aceptar en la red lo autorizado y lo demás denegado, se debe tomar en cuenta los firewall entre los servidores y servicios.
Los logs son indispensables para obtener resultados inmediatos que busca el auditor puesto que algunos test son analizado, quien no ha revisado los logs, (HERZOG PETE, 2003,p. 60)

13. El Cortafuegos y sus características.

Como objeto tiene verificar el tipo de router que utiliza el tipo de servicio que ofrece sus instrucciones con opciones TTL; prueba ACL de cortafuegos comprueba filtrado de tráfico hacia afuera, detección de direcciones, escaneo inverso en el módulo; Testear las capacidades externas, establece métodos de investigación; también la posibilidad de escanear SYN y puertos específicos.

Más características de cortafuegos son como la cuantificación para fragmentar en ataques del tipo TEARDROP; paquetes diminutos y realizar pruebas de paquetes entrantes (inundación) de los paquetes RST, UDP, ACK, FIN, NULL, WIN, XMAS
Verificar la habilidad de los cortafuegos para protegerse de varias técnicas usando IPIDs, (HERZOG PETE, 2003,p. 61)

14. Testeo de Sistema de Detección de Intrusos

La prueba se encamina a los beneficios y al rendimiento del IDS esta prueba no se puede llevar a cabo si no existen registros IDS, las pruebas suelencorresponder a ataques de ancho de banda, saltos distantes, y latencia que afectan al resultado de estos test.Algunos que son desconocidos son destinados para el analista, quien no ha revisado los registros y alertas , (HERZOG PETE, 2003,p. 62)

El IDS y sus características
1. Verifica determina explota configura los parámetros la velocidad y la explotación de IDS.

2. Prueba la configuración del IDS para las velocidades, durante un ataque, cambios aleatorios de protocolos, aleatorios de origen puerto de origen manejo de paquetes métodos de ataques
3. Testear los efectos y reacciones del IDS. Una dirección IP contra varias direcciones.
4. Encontrar alertas de IDS sobre escaneos de vulnerabilidades, alertas de IDS sobre descifrado de contraseñas, alertas de IDS de testeos de sistemas confiados.

15. Testeo de Medidas de Contingencia

Las medidas de contingencia dictan el manejo de lo atravesale, programas maliciosos y emergencias, la identificación de los mecanismos de seguridad y las políticas de respuesta que necesiten ser examinados. Debe ser necesario responder primero a una nueva cuenta de correo electrónico de pruebas o al sistema de escritorio donde el administrador pueda monitorizar, , (HERZOG PETE, 2003,p.63)

16. Descifrado de Contraseñas

El fuerte de esta prueba es que no descifren contraseñas códigos personal ajeno se debe contar con robustez todas las contraseñas en su mayoría de veces los atacantes utilizan fuerza

Para obtener la información original para los atacantes puede ser algo simple con la ayuda de herramientas , también subrayar la necesidad del refuerzo de una política estricta de contraseñas de usuario, generación automática, o módulos del tipo PAM , (HERZOG PETE, 2003,p. 64)

17. Testeo de Denegación de Servicios

Los test de DoS reciban ayuda adicional de la organización y sea monitorizada a nivel privado. Inundación y ataques DoS Distribuidos (DDoS) están específicamente no comprobados y prohibidos por este manual, los ataques de inundación y los ataques DDoS SIEMPRE causarán ciertos problemas y a veces no solamente al objetivo sino también a los enrutadores y sistemas entre el auditor y el objetivo, , (HERZOG PETE, 2003,p. 65)

Evaluación de Políticas de Seguridad

La evaluación de políticas de seguridad se sigue las siguientes técnicas:
Cotejar las políticas de seguridad, que la política sea aprobada por la gerencia, certificar la documentación y que la política sea leída y aceptada por el personal que pueda obtener a los sistemas.

1. Identifique los procedimientos de manejo de incidentes, para asegurarse de que las brechas de seguridad son manejadas por las personas adecuadas y que son reportadas de manera apropiada
2. Conexiones entrantes – Verifique los riesgos mencionados que tienen relación directa con las conexiones entrantes de Internet (Internet -> DMZ, Internet -> red interna), y las medidas que son necesarias implementar para reducir o eliminar dichos riesgos. Estos riesgos pueden ser permitidos en conexiones entrantes, típicamente SMTP, POP3, HTTP, HTTPS, FTP, VPNs y las correspondientes medidas como esquemas de autenticación, encriptación y Listas de Control de Acceso.
3. Conexiones salientes– Las conexiones salientes pueden producirse entre la red interna y DMZ, así como también entre la red interna e Internet. Busque cualquier regla de conexiones salientes que no se corresponda con la implementación. Las conexiones salientes no pueden ser usadas para introducir código malicioso o revelar las especificaciones de la red interna.
4. Medidas de seguridad– Las reglas que exigen la implementación de medidas de seguridad, deben ser cumplidas. Aquellas pueden hacer uso de AVS, IDS, cortafuegos, DMZs, routers y las configuraciones/implementaciones adecuadas de acuerdo con los riesgos a contrarrestar.
5. Comprobar la política de seguridad contra el estado actual de las conexiones no relacionadas a Internet.
6. Modems– Debe existir una regla que indique que el uso de modems que no están especialmente asegurados está prohibido o al menos sólo permitido si los modems están desconectados cuando no se encuentran en uso, y configurados para no permitir el marcado. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.
7. Máquinas de Fax– Debe existir una regla que indique que el uso de las máquinas de fax que pudiera permitir acceso desde el exterior a la memoria de las

máquinas, está prohibido o al menos sólo permitido si las máquinas son apagadas cuando no se las utiliza. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.

8. PBX– Debe existir una regla que indique que la administración remota del sistema PBX está prohibida o al menos sólo permitida si las máquinas son apagadas cuando no se las utiliza. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.

9. Verifique que la política de seguridad establezca las medidas de contención y los test de ingeniería social basados en el uso indebido de Internet por parte de los empleados, de acuerdo con la justificación de negocios y las mejores prácticas de seguridad , (HERZOG PETE, 2003,p. 66)

CAPITULO III

3. METODOLOGÍA OSSTMM APLICADO A DETECCION DE VULNERABILIDADES IPv6

3.1 Introducción

OSSTMM es un manual para análisis, pruebas de seguridad informática, lo que implica que sea una metodología extensa, además de no tener un enfoque específico para ciertas áreas de una infraestructura completa de dato, por otra parte IPv6 es una nueva tecnología para la interconectividad de redes misma que presenta muchos errores de seguridad motivo por el cual la mayoría de empresas, organizaciones, instituciones, etc. no han optado por una migración completa a esta tecnología. Hay que recalcar que existen otros motivos además de los de seguridad y son los económicos ya que todas las infraestructuras al momento tienen todos sus equipos para IPV4 lo que resulta un coste elevado el cambio de equipos, otro aspecto a tomar en cuenta es que al momento los fabricantes de software como hardware para redes no se han centrado completamente en IPv6.

Por todo lo mencionado anteriormente nace la imperiosa necesidad de crear un Framework o una metodología basada en OSSTMM y enfocarla en análisis, pruebas y de ser posible en corrección de vulnerabilidades en infraestructuras IPv6.

3.2 Metodología.

En la presente investigación se utilizará el método científico debido a que se logrará determinar los criterios y/o procedimientos en base a la metodología OSSTMM para la estructuras IPV6.

Esta metodología divide la totalidad de una infraestructura en seis secciones:
Sección A -Seguridad de la Información
Sección B – Seguridad de los Procesos
Sección C – Seguridad en las tecnologías de Internet
Sección D – Seguridad en las Comunicaciones

Sección E – Seguridad Inalámbrica

Sección F – Seguridad Física

Para la realización de este proyecto se toma en consideración la sección C de la Metodología OSSTMM que dice lo siguiente:

1. Logística y Controles
2. Exploración de Red
3. Identificación de los Servicios del Sistema
4. Búsqueda de Información Competitiva
5. Revisión de Privacidad
6. Obtención de Documentos
7. Búsqueda y Verificación de Vulnerabilidades
8. Testeo de Aplicaciones de Internet
9. Enrutamiento
10. Testeo de Sistemas Confiados
11. Testeo de Control de Acceso
12. Testeo de Sistema de Detección de Intrusos
13. Testeo de Medidas de Contingencia
14. Descifrado de Contraseñas
15. Testeo de Denegación de Servicios
16. Evaluación de Políticas de Seguridad

3.*2.1* ***Propuesta de la metodología para análisis de vulnerabilidades en infraestructuras IPv6.***

Basados en la Metodología OSSTMM se propone la siguiente metodología para análisis de Vulnerabilidades en infraestructuras con direccionamiento IPv6.

1. Análisis y Evaluación de Riesgos en Infraestructuras con Direccionamiento IPv6.

a. Riesgos Tecnológicos.
b. Riesgos Económicos.
c. Riesgos de seguridad de la información.

2. Identificación y Búsqueda de Vulnerabilidades IPV6.

a) Descubrimiento de direcciones IPv6.
b) Detección de Servidores IPv6

c) Escaneo de puertos y servicios que corren en la infraestructura IPv6.

d) Ataques IPv6.

e) Explotación.

3. Informe del Análisis, Valoración y posible tratamiento de riesgos sobre las vulnerabilidades encontradas en infraestructuras IPv6.

Matriz de análisis de vulnerabilidades.

Tabla 1-3 Matriz de Análisis de Vulnerabilidades

Ataque realizado	Criterio de seguridad afectado	Herramienta utilizada	Valoración
Descubrimiento de direcciones locales IPv6 mediante búsqueda en segmentos de red ipv4	Confidencialidad	atk6-alive6 -4 192.168.1.0/24 eth0	Low
Detección de nuevas direcciones IP	Confidencialidad	atk6-detect-new-ip6 eth0	Low
Detección de servidores de DHCPv6	Confidencialidad	atk6-dump_dhcp6 eth0	Medium
Detección de routers	Confidencialidad	atk6-dump_router6 eth0	Medium
Escaneo de Puertos	Confidencialidad	nmap -6 2001:db8:1:40::3 --open -O	Medium
Ataque de Fragmentación de Paquetes	Disponibilidad	atk6-fragmentation6 eth0 2001:db8:1:10::2	Medium
Ataque ICMPv6 Smurf	Disponibilidad	atk6-smurf6 eth0 2001:db8:1:40::2	High
Denegación de Servicio hibrido dirigido hacia los routers	Disponibilidad	atk6-denial6 eth0 2001:db8:1:40::2 1	High
Denegación de Servicio hibrido hacia la victima	Disponibilidad	atk6-denial6 eth0 2001:db8:1:40::2 2	High
Explotación de vulnerabilidades en IPv6	Disponibilidad	atk6-exploit6 eth0 2001:db8:1:40::2 1	Medium
Explotación de vulnerabilidades en IPv6	Disponibilidad	atk6-exploit6 eth0 2001:db8:1:40::2 2	Medium
Explotación de vulnerabilidades en IPv6	Disponibilidad	atk6-exploit6 eth0 2001:db8:1:40::2 3	Medium
Denegación de servicio global	Disponibilidad	atk6-flood_router26 eth0	High
Análisis de Vulnerabilidades	Integridad, Confidencialidad, Disponibilidad	Nessus	High
Generación de Payloads mediante tunneling IPv6	Integridad, Confidencialidad, Disponibilidad	msfvenom	High
Ataques Client Side	Integridad, Confidencialidad, Disponibilidad	Metasploit	High

Ataques de Intercepción de tráfico	Integridad, Confidencialidad, Disponibilidad	atk6-parasite6 eth0	High

Realizado por: Martínez, Carlos, 2015

3.2.2 Evolución de infraestructura.

Análisis y Evaluación de Riesgos en Infraestructuras con Direccionamiento IPv6.

Antes de iniciar un test de seguridad o una auditoria de seguridad primeramente se debe hacer una evaluación de la infraestructura en los siguientes aspectos:

a. Riesgos Tecnológicos.

Una empresa, institución, etc. indistintamente de la actividad que realice, implica que tiene implementado en su infraestructura equipos hardware (servidores, wireless, equipos de almacenamiento de la información, dispositivos de red, etc.) y software (sistemas operativos, servidores de base de datos, servidores de aplicaciones, servidores web, proxy, etc.). Esta evaluación permitirá identificar el coste tanto hardware o software y los posibles errores que se podrían causar debido al test de seguridad.

b. Riesgos Económicos.

Aquí es importante tomar en cuenta la actividad económica o de servicio a la que se dedica la empresa, institución, etc. debido a la perdida que puede implicar si se suspende el servicio cuando se realice la auditoria de seguridad por tanto es recomendable evaluar este riesgo para elabora un plan que incluya un cronograma en fechas u horas que no se realice la actividad económica de servicios.

c. Riesgos de seguridad de la información.

Hay que tener mucho en cuenta este aspecto debido a la confidencialidad de la información que maneje la empresa, institución, etc. a la que se realiza la auditoria, por tanto, es menester preocuparse de este punto ya que se puede perder la información o puede haber una fuga de la misma.

Identificación y Búsqueda de Vulnerabilidades ipv6.

Como se sabe para un hacking se sigue las siguientes fases:

- Reconocimiento

- Escaneo
- Obtener acceso
- Borrar huellas.

Según lo anterior en este punto se realiza la auditoria en sí de la siguiente manera. Primero se realiza un reconocimiento de las direcciones locales de red en IPv6, luego se realiza una escaneo de servidores en IPv6, posteriormente detección de Routers de Bordes, después un escaneo de puertos. Una vez recopilada esta información se procede a los ataques para comprobar las vulnerabilidades y posteriormente a la explotación de ciertas vulnerabilidades persistentes en IPv6.

Para lograr este cometido de una manera fácil se adjunta a la metodología un paquete para correr en un sistema Operativo Linux conjuntamente con el paquete THC-IPv6-Attack-Toolkit que permite realizar todo este proceso de una manera automatizada.(anexo1)

Descubrimiento de direcciones IPv6.
Detección de Servidores IPv6
Escaneo de puertos y servicios que corren en la infraestructura IPv6.
Ataques IPv6.
Explotación

- **Informe del Análisis, Valoración y posible tratamiento de riesgos sobre las vulnerabilidades encontradas en infraestructuras IPv6.**

Las Vulnerabilidades que sean encontradas serán analizadas en primer lugar según su tiempo de aparición es decir si ya hay un parche de seguridad o es Zero-day podrán ser catalogadas como (high - medium - low) y su potencial para causar o comprometer la información en: Confidencialidad – Disponibilidad – Integridad). Para fines de la metodología se ha desarrollado una matriz para la comparación de vulnerabilidades encontradas con las persistentes en IPv6.

3.3.3 Requerimientos

Los siguientes instrumentos publicados a continuación son los usados para la realización de este trabajo de investigación.

Tabla 2-3 Requerimientos de la Investigación

INSTRUMENTO	CARACTERISTICAS
Kali Linux	386i versión 2.3 -2015
THC-IPv6	V2.7
VMware Workstation	
Windows7	64bits
WindosXP	64bits
Elastix_IPv6	V5.9
GNS3 opensource	V1.4
IOS Cisco	V12.4
Nessus	
Wireshark	V1.12.1

Realizado por: Martínez, Carlos, 2015

3.3.4 Validación de Instrumentos.

Se utiliza Kali Linux ya que es una distribución basada en Debian GNU/Linux especializada para pruebas de penetración y seguridad informática. Kali Linux es comparada con una caja de herramientas del profesional de seguridad (hacker). Dispone de más de 600 herramientas para las pruebas y auditorias, muchas de ellas son orientadas a análisis de infraestructuras de datos viene en su versión para IPV4 como también en IPv6 que justamente se usan en este trabajo investigativo, otra característica es que como está desarrollado bajo un Kernel de Linux permite instalar herramientas y paquetes adicionales de otras distribuciones.

1. THC-IPv6 acrónimo de The Hacker's Choice, es un conjunto de herramientas para explotar vulnerabilidades en ambientes netamente con IPv6, como esta investigación se basa en eso, esta herramienta resulta de gran importancia para la realización del este proyecto.

2. WMware Workstation, el uso de este software permite correr diferentes sistemas operativos en una maquina con un sistema operativo anfitrión es decir los virtual iza, dándonos la posibilidad de usar Linux sin tener la necesidad de poseer un equipo físico para el caso.

3. Windows XP, surge la necesidad de usar este sistema operativo debido a que su uso aun es necesario por la existencia de aplicaciones en el mundo de los negocios y de las fábricas que corren bajo este sistema operático que a pesar ya del abandono por parte de Microsoft a este proyecto aún está muy enraizado en algunos ámbitos del negocio.

4. Elastix_IPv6, el uso de telefonía y servicios asociados se ha tornado una necesidad básica en el ámbito de los negocios, educación, empresarial, estado, por tanto se vio la necesidad de implementar un servidor de voz como lo es elastix cargado con todos los paquetes para que pueda soportar la versión de IPv6.

5. GNS3**,**opensource es un simulador grafico de red, permite tener todas las características de una entorno físico real, como el laboratorio de cisco no posee una amplia infraestructura para el desarrollo de esta investigación surge la necesidad de elabora un ambiente de simulación con una granja de servidores todo esto en GNS3.

6. IOS Cisco, como se manifestó anteriormente se usa GNS3 opensource y para simular de una forma casi real los equipos CISCO es necesario la adquisición de un IOS v12.4 la última versión que corren en cada equipo de esta marca.

7. NESSUSes un escáner de vulnerabilidades que posee módulos de IPv6 para correr sobre infraestructuras con esta característica.

8. Wireshark tiene la funcionalidad de trabajar como un analizador de paquetes de red, muy útil en esta investigación para poder examinar los paquetes que son vulnerables así como para ver cómo está infectada una red cuando se lanza un ataque.

9. Nmap **6**, es una utilidad para el descubrimiento de componentes de una infraestructura de red y como podeos observar que al final de la palabra nmap tenemos

el numero 6 eso hace referencia a que está desarrollado básicamente para entornos con direccionamiento IPv6.

3.*4 Ambiente de pruebas.*

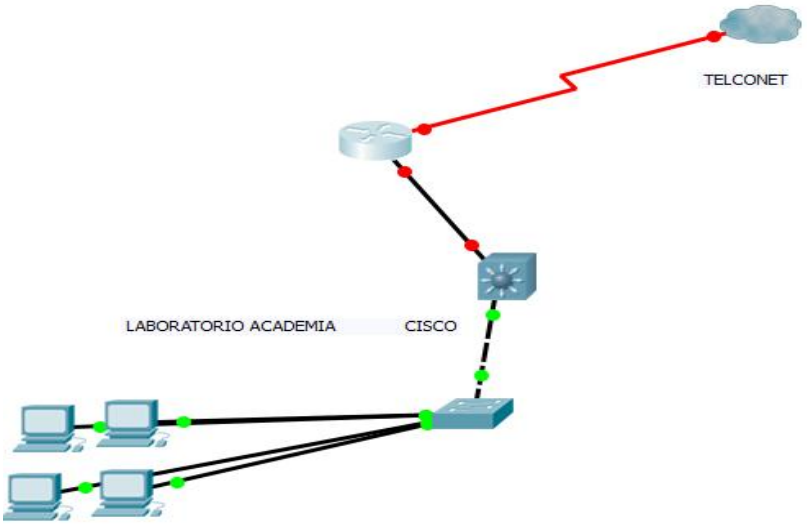


Figura 1-3 Ambiente de pruebas
Realizado por: Martínez, Carlos, 2015

Análisis

Como se puede observar en la ilustración 24, el laboratorio de CISCO tiene los equipos básicos en lo que se refiere a IPv6 por lo que surge la necesidad de implementar un ambiente de pruebas controlado debido a que en esta infraestructura se incluyen otros laboratorios que están en uso las 8 horas laborables, no se da un direccionamiento de la infraestructura de la Academia CISCO por motivos de seguridad al ser esta investigación pública.

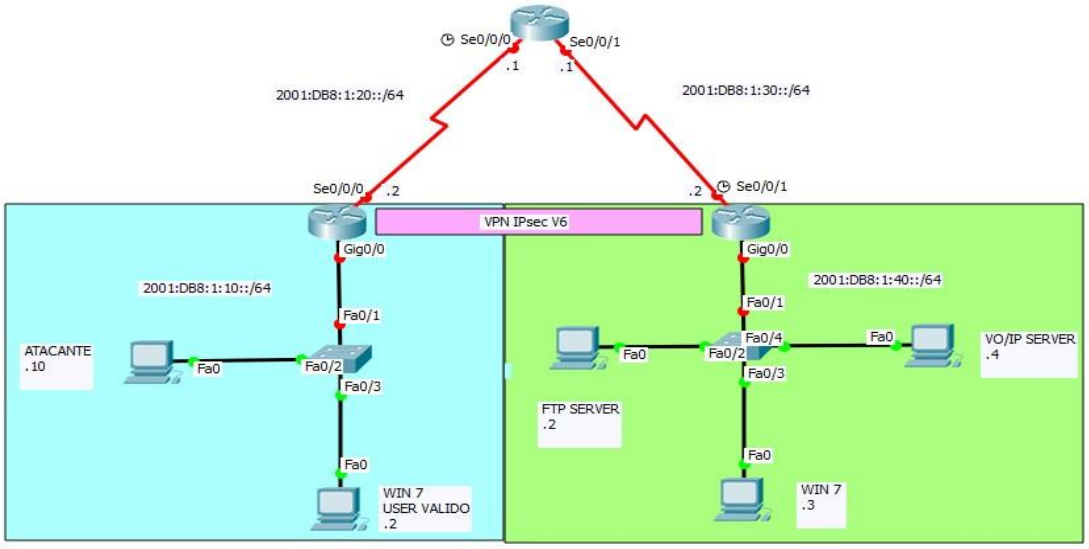


Figura 2-3 Direccionamiento del laboratorio CISCO
Realizado por: Martínez, Carlos, 2015

Análisis

Un aspecto muy importante a tomar en cuenta es que el atacante va a estar fuera de la red y se debe medir las vulnerabilidades existentes desde ese ámbito y dentro de la red por eso en el grafico se muestra un túnel VPN IPsec V6 mismo que simula el internet para separar las dos infraestructuras en donde la una es la granja de servidores que constan de un servidor FTP, un servidor de VO/IP un WIN7 en donde corren servicios convencionales usados en una red de datos. Todo esto se ha simulado en GNS3.

CAPITULO IV

4. APLICACIÓN DE LA METODOLOGÍA EN EL LABORATORIO DE CISCO DE LA ESPOCH

4.1 Pruebas

4.1.1 Preparación de los instrumentos.

Para el caso como se menciona anteriormente el ambiente de pruebas está diseñado y creado en GNS3, programa que permite desarrollar infraestructuras similares a las reales.

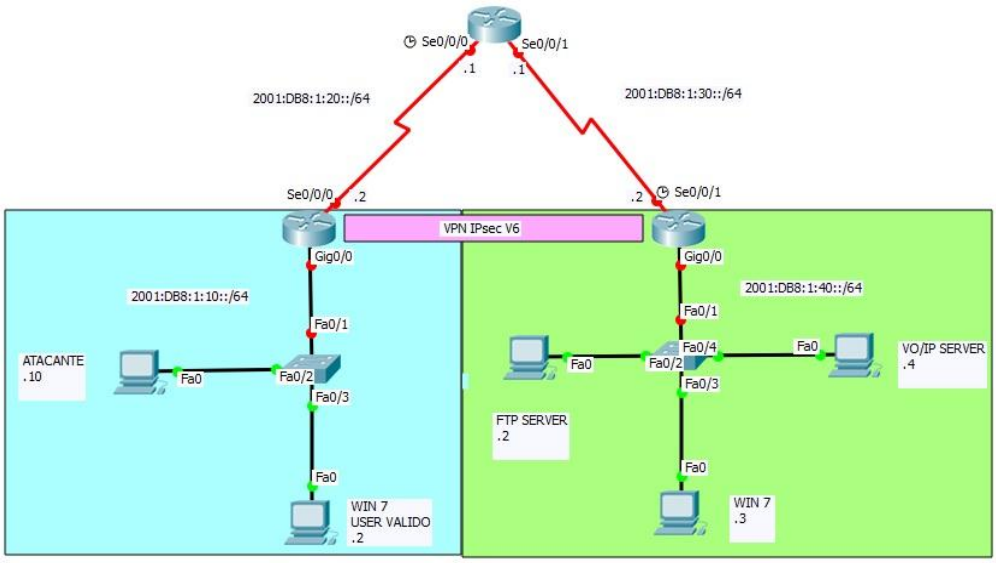


Figura 1-4 Preparación de instrumentales
Realizado por: Martínez, Carlos, 2015

Después se procede a montar los servidores iniciando por un de VoIP en IPV6, para lo que se usa Elastix con todos los módulos para IPV6.

Figura 2-4 Instalación de Elastix
Realizado por: Martínez, Carlos, 2015

Luego de todo el proceso de instalación se procede a la configuración de red del servidor.

Figura 3-4 Configuración del servidor
Realizado por: Martínez, Carlos, 2015

Después se procede a instalar Kali Linux

Figura 4-4 Instalación de Kali Linux
Realizado por: Martínez, Carlos, 2015

Después de instalar tenemos que actualizar todos los módulos IPv6 además de instalar

VMwareTools debido a que estamos virtualizando, para proceder al análisis de Vulnerabilidades.

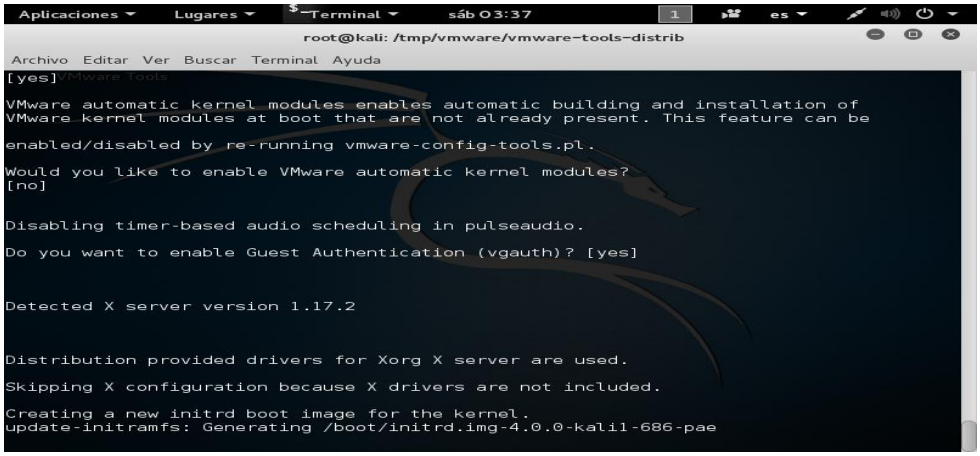


Figura 5-4 Actualización de módulos IPv6
Realizado por: Martínez, Carlos, 2015

DESARROLLO

4.2.1 Análisis y evaluación de riesgos en el laboratorio CISCO DE LA ESPOCH.

a) Riesgos Tecnológicos.

En el departamento de Cisco no existe ningún riesgo de este tipo ya que en si la infraestructura en IPv6 no es completa y por consiguiente el ambiente de prueba que se desarrolló para el caso de estudio no representa o más bien no presenta ninguna pérdida Tecnológica.

b) Riesgos Económicos.

Por lo anotado anteriormente existe un riesgo económico por llamarlo así ya que la academia CISCO se dedica a desarrollar un programa de preparación de estudiantes y profesionales a través de clases presenciales y de uno de los modelos e-learning más avanzados del mundo, ya sea en diseño, configuración, monitoreo y mantenimiento de redes, cuando se utilizaba el laboratorio para las pruebas los fines de semana, habían estudiantes haciendo uso de la demás infraestructura de cisco por lo que fue menester buscar horarios cómodos en los que no interfiera con la presencia de estudiantes debido

a que ciertos ataques hacen que colapsen los procesadores de servidores y equipos de cómputo dejándolos sin poder usarlos hasta que sean reiniciados.

Horario para pruebas días Domingos de 8:00 a 12:00.

c) Riesgos de Seguridad de la Información.

Por la actividad a la que se dedica la academia CISCO no presenta información confidencial o que se pueda comprometer.

4.2.2 Identificación y búsqueda de vulnerabilidades IPv6.

Se procede a ejecutar el script del programa que llama a todas las librerías TCHIPv6.

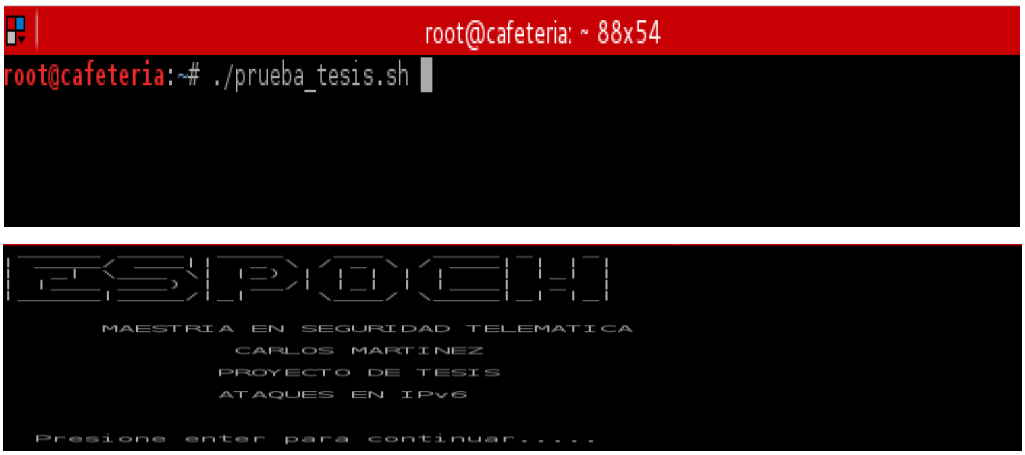


Figura 6-4 Pantalla de inicio del Script
Realizado por: Martínez, Carlos, 2015

4.2.3 Descubrimiento de direcciones ipv6.

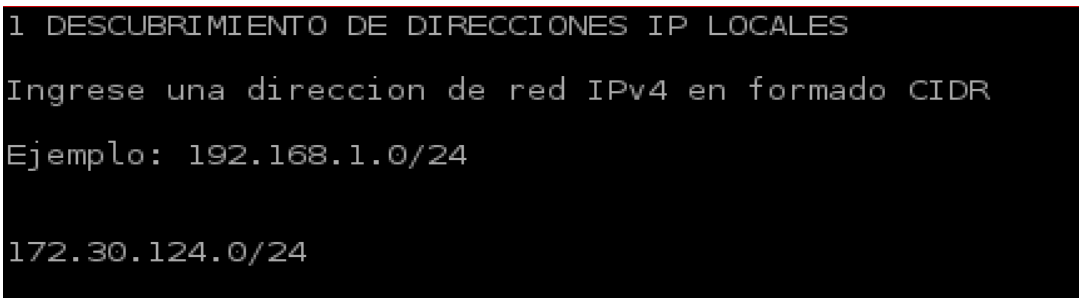


Figura 7-4 Descubrimiento de direcciones IP locales
Realizado por: Martínez, Carlos, 2015

El descubriendo de direcciones locales IPv6 se hace mediante búsqueda en segmentos de red ipv4 (atk6-alive6 -4 192.168.1.0/24 eth0) esta herramienta es posible enviar paquetes ICMPv6 a direcciones de multicast FF02::1, con lo cual todos los dispositivos que se encuentren habilitados IPv6 responderán al paquete ICMPv6 indicando su dirección global.

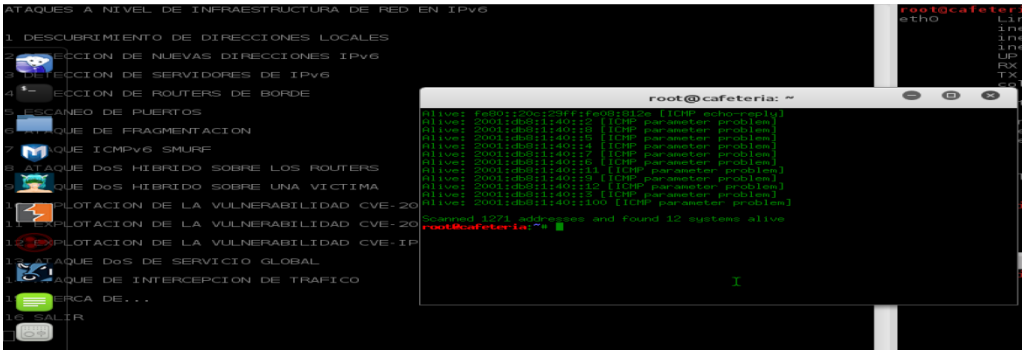


Figura 8-4 Menú del script
Realizado por: Martínez, Carlos, 2015

4.2.4Detección de nuevas direcciones ip (atk6-detect-new-ip6 eth0),

Por defecto cuando un nuevo host es agregado a la red mediante IPv6, envía solicitudes de neighbor Discovery, con lo cual si un atacante inicia un sniffer, es capaz de capturar tanto la nueva dirección de link-local así como la dirección de global-link, además la herramienta permite adicionar un script que puede ser ejecutado cuando se detecte una nueva dirección que se añadido al segmento de red local.

Detección de Servidores**.**

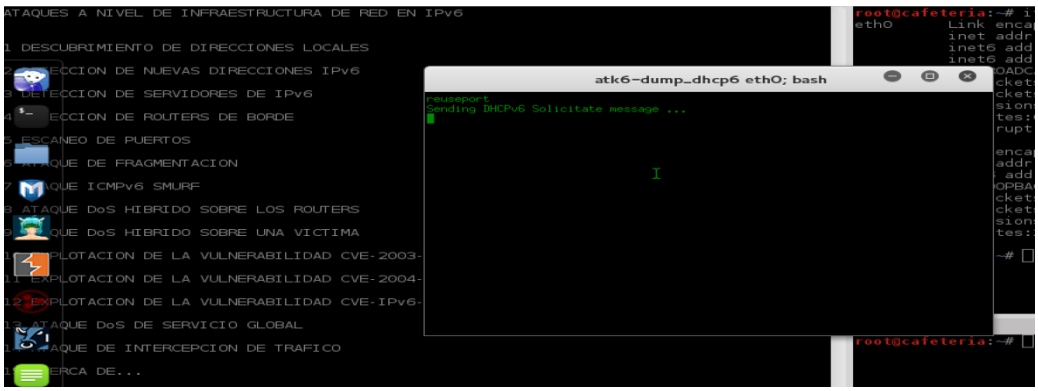


Figura 9-4 Detección de servidores
Realizado por: Martínez, Carlos, 2015

Detección de servidores de DHCPv6 (atk6-dump_dhcp6 eth0), la herramienta permite descubrir los servidores de DHCPv6 que se encuentren habilitados en el segmento de

red local, lo cual atenta a la confidencialidad de la información, por cuanto un atacante podría generar un ataque de denegación de servicio sobre el servidor DHCP y suplantar la identidad del mismo con parámetros erróneos que le permitirían controlar la asignación de direcciones IP.

Detección de routers (atk6-dump_router6 eth0), permite detectar los routers conectados en el segmento de red local, lo cual atenta contra la confidencialidad de la información.

4.2.5 Escaneo de puertos y servicios que corren en la infraestructura.

Para tal cometido se presiona el número 5 y se da la dirección de la víctima que se desea indagar, esta dirección apareció en los pasos anteriores.

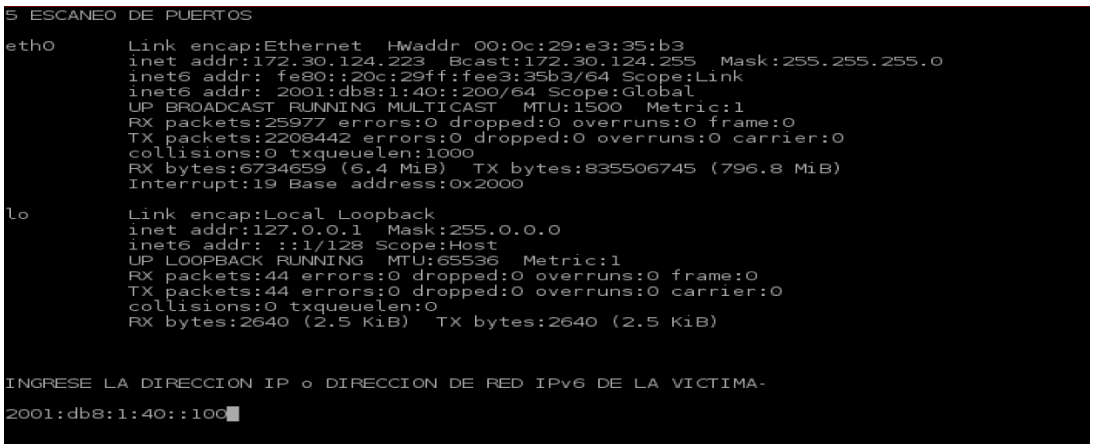


Figura 10-4 Escaneo de Puertos
Realizado por: Martínez, Carlos, 2015

Escaneo de Puertos (nmap -6 2001:db8:1:40::100 --open –O),mediante la ejecución de Nmap, es posible determinar el estado operativo en el cual se encuentra un puerto respecto al servicio brindado, además es posible determinar el tipo de sistema operativo de la víctima y numero de saltos que debe atravesar el atacante hasta llegar a su objetivo, de esta manera el atacante está en la capacidad de conocer los dispositivos de capa 3 que realizan forwarding de sus paquetes pudiendo inclusive realizar ataques sobre estos routers.

Figura 11-4 Estado operativo de los puertos
Realizado por: Martínez, Carlos, 2015

.

4.2.6 Ataques IPv6.

Una vez que se recolecta la información necesaria de la infraestructura de red en IPv6 se procede a realizar los siguientes ataques.

Ataque de fragmentación.

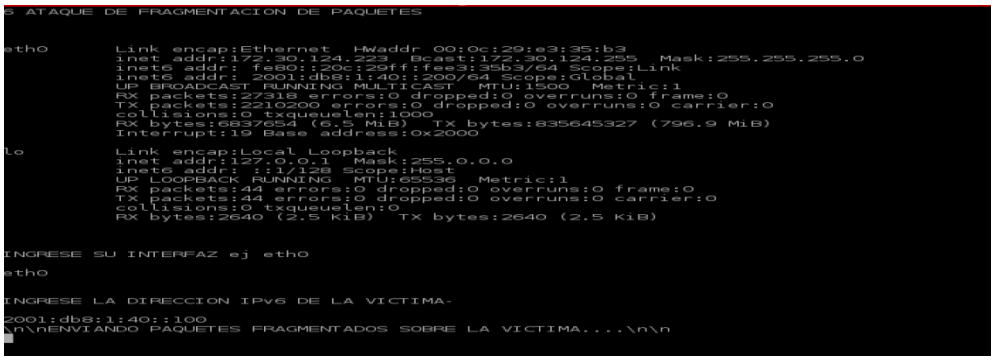


Figura 12-4 Ataques por fragmentación
Realizado por: Martínez, Carlos, 2015

Ataque de Fragmentación de Paquetes (atk6-fragmentation6 eth0 2001:db8:1:10::2) , por defecto mediante la utilización de IPv6 los routers y dispositivos de capa 3 no fragmentan los paquetes cundo son enviados desde sus interfaces, sin embargo mediante el uso de la herramienta frag6, es posible crear una fragmentación de los paquetes que son enviados a un host final, mediante esta técnica, el atacante está en la posibilidad de enviar paquetes con distintos tamaños a la víctima, evadiendo medidas de seguridad implementadas en soluciones IDS, cuando la víctima recibe el ataque, necesita agregar recursos de memoria a los buffers creados para la

recepción de cada paquete, el incremento en la memoria asignada genera una baja de recursos, lo que atenta a la disponibilidad de la información.

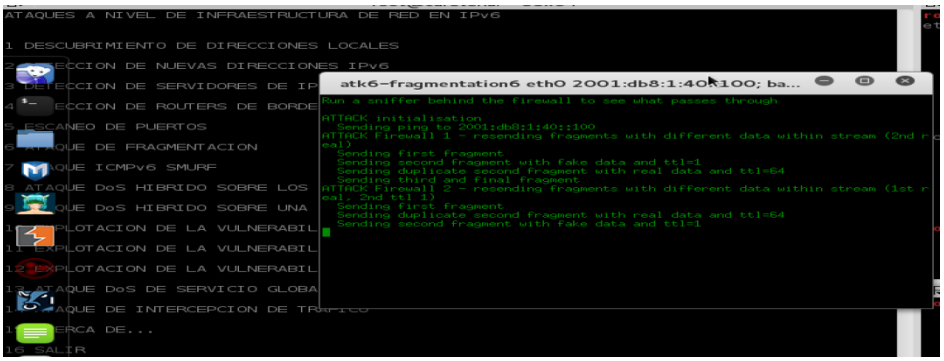


Figura 13-4 Ataque de Fragmentación de Paquetes (atk6-fragmentation6 eth0 2001:db8:1:10::2)
Realizado por : Investigador (MARTINEZ CARLOS,2015)

Ataque icmpv6 SMURF

Para este ataque se presiona la tecla 7, se escribe la interfaz por donde va a lanzar el ataque, en este caso eth0, procedemos aingresar la dirección IPv6 de la víctima.

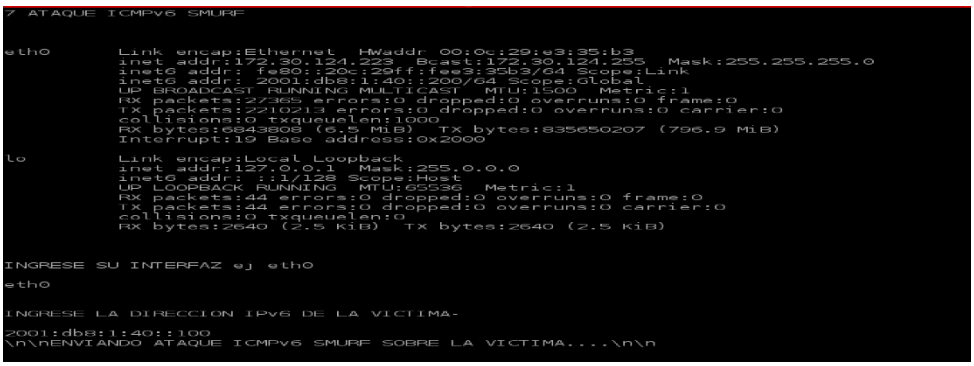


Figura 14-4 Ataque ICMPv6 SMURF
Realizado por : Investigador (MARTINEZ CARLOS,2015)

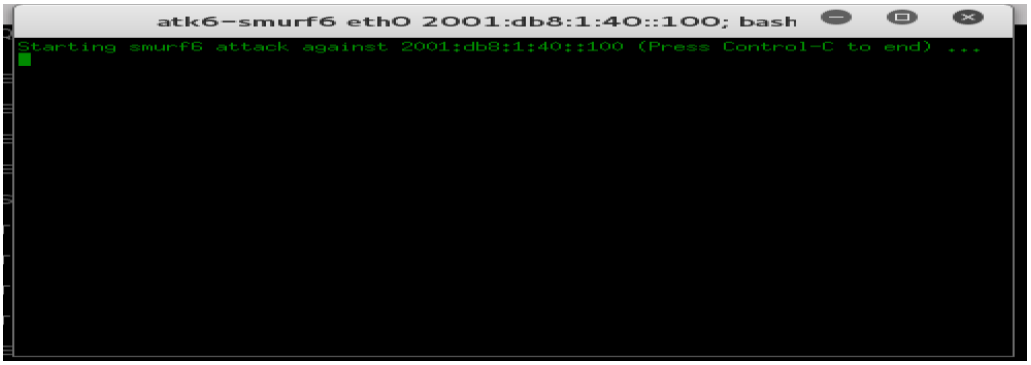


Figura 15-4 Atk6-smurf6 eth0 2001:db8:1:40::100
Realizado por: Martínez, Carlos, 2015

Ataque icmpv6 Smurf (atk6-smurf6 eth0 2001:db8:1:40::2) Envía solicitudes echo ICMPv6 a todas las direcciones de multicast disponibles, como resultado todos los dispositivos re envían trafico ICMPv6 a la víctima.

Ataque DoS hibrido sobre los routers**.**

Para este ataque se presiona la tecla 8, se escribe la interfaz por donde va a lanzar el ataque, en este caso eth0, procedemos aingresar la dirección IPv6router víctima.

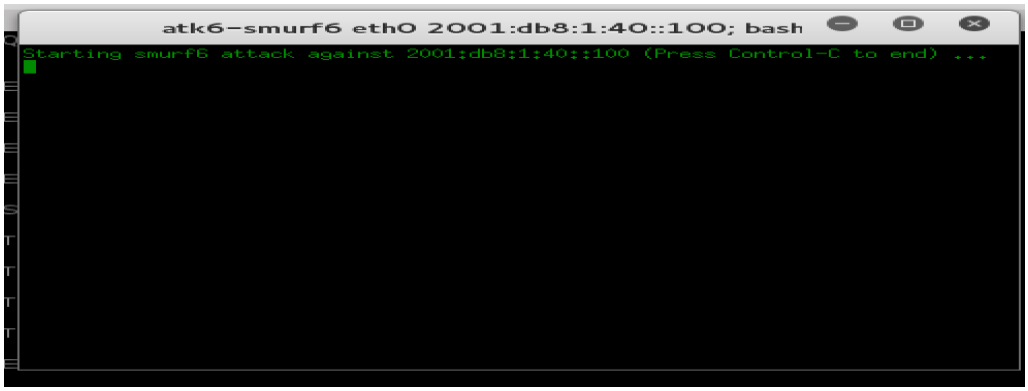


Figura 16-4 Ataques híbridos
Realizado por: Martínez, Carlos, 2015

Denegación de Servicio hibrido dirigido hacia los routers (atk6-denial6 eth0 *2001:db8:1:40::2 1)*, genera una gran cantidad de solicitudes icmpv6, route advertisement y neighbor advertisement, lo cual atenta a la disponibilidad de todos los routers que se encuentren en el path hacia la victima

Ataque DoS hibrido sobre la víctima.

Para este ataque se presiona la tecla 9, se escribe la interfaz por donde se va a lanzar el ataque, en este caso eth0, procedemos aingresar la dirección IPv6 de la víctima.

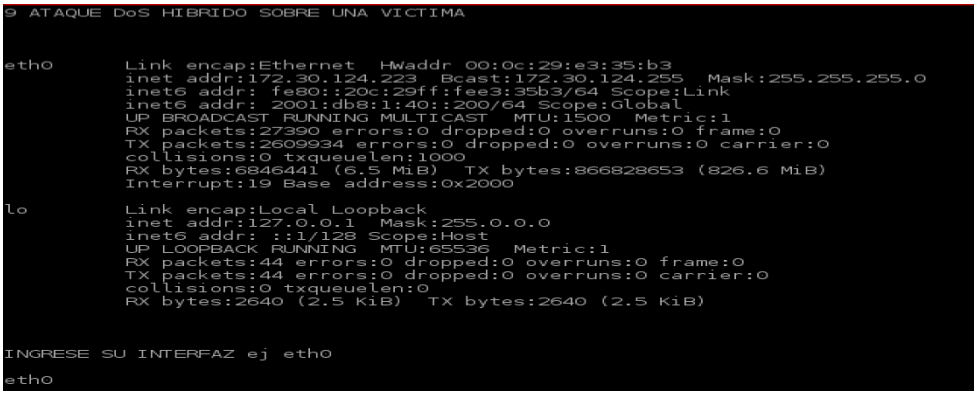


Figura 17-4 Ataques DoS Hibrido sobre una victima
Realizado por: Martínez, Carlos, 2015

Denegación de Servicio hibrido hacia la victima (atk6-denial6 eth0 2001:db8:1:40::2 ***2)***,genera una gran cantidad de solicitudes icmpv6, route advertisement y neighbor advertisement hacia la víctima del ataque, no afecta a los dispositivos de networking que se encuentran en el path.

Explotación de la vulnerabilidad CVE-2003-0429.

Para este ataque se escribe el número 10, se escribe la interfaz por donde se va a lanzar el ataque, en este caso eth0, procedemos aingresar la dirección IPv6 de la víctima.

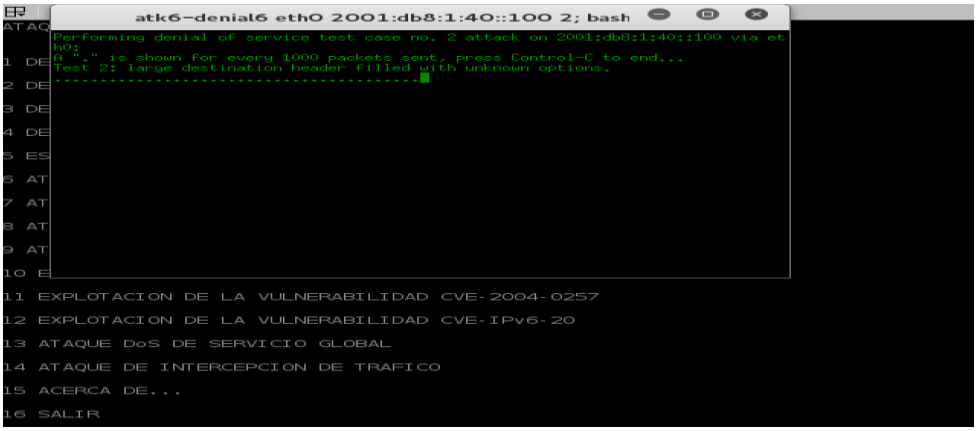


Figura 18-4 Explotación de vulnerabilidades CVE-2004-0257
Realizado por: Martínez, Carlos, 2015

Explotación de vulnerabilidades en IPv6 (atk6-exploit6 eth0 2001:db8:1:40::2

1)Explota la vulnerabilidades CVE-2003-0429 que generaría una denegación de servicio por él envió excesivo de prefijos de red que no se rigen el estándar. Para ejecutar la explotación de las siguientes vulnerabilidades es importante conocer si la infraestructura es o no endeble a las mismas. Para saber es necesario correr Nessus en con paquetes IPv6.

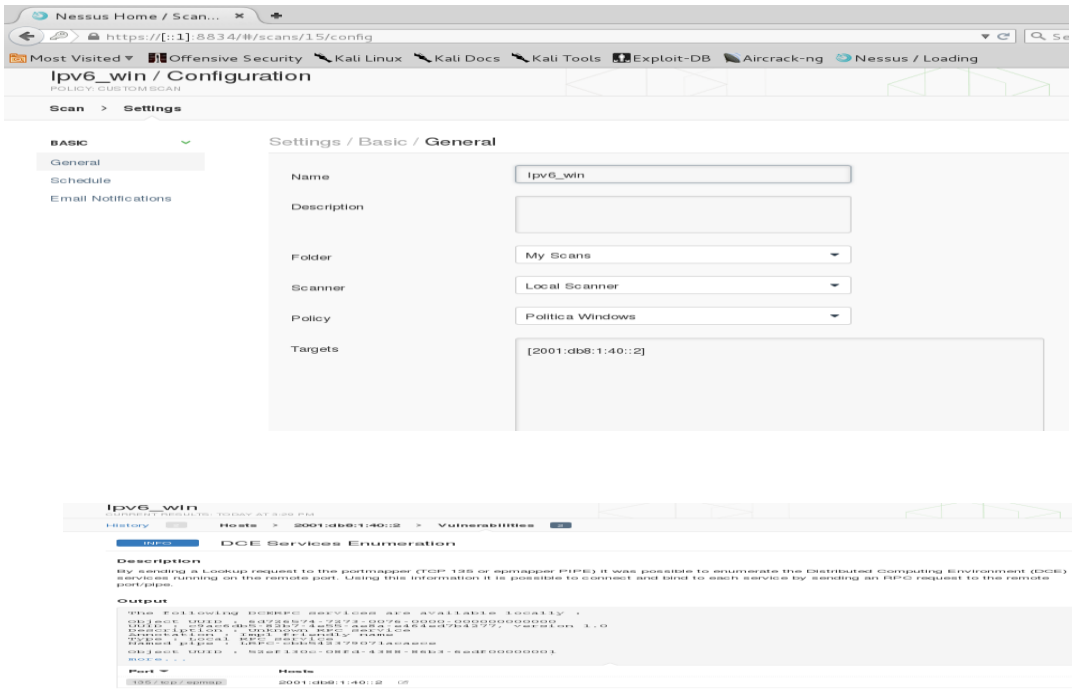


Figura 19-4 Explotación de vulnerabilidades en IPv6
Realizado por: Martínez, Carlos, 2015

Explotación de la Vulnerabilidad CVE-2004-0257

Para este ataque se escribe el número 11, se escribe la interfaz por donde se va a lanzar el ataque, en este caso eth0, procedemos aingresar la dirección IPv6 de la víctima.

Figura 20-4 Explotación de la Vulnerabilidad CVE-2004-0257 en el 11
Realizado por: Martínez, Carlos, 2015

Explotación de vulnerabilidades en IPv6 (atk6-exploit6 eth0 2001:db8:1:40::2 2) Explota la vulnerabilidad CVE-2004-0257 que generaría una denegación de servicio por el flooding de solicitudes TCP SYN mediante el envío de paquetes fuera del tamaño estándar.

Explotación de la vulnerabilidad CVE-ipv6-20

Para este ataque se escribe el número 12, se escribe la interfaz por donde se va a lanzar el ataque, en este caso eth0, procedemos aingresar la dirección IPv6 de la víctima.

Figura 21-4 Explotación de la vulnerabilidad CVE-IPv6-20
Realizado por: Martínez, Carlos, 2015

Explotación de vulnerabilidades en IPv6 (atk6-exploit6 eth0 2001:db8:1:40::2 3) Explota la vulnerabilidad CVE-20 que genera una denegación de servicio por el envío excesivo de paquetes router advertisement.

Ataque de servicio Global

Para este ataque se escribe el número 13, se escribe la interfaz por donde se va a lanzar el ataque, en este caso eth0 e inicia el ataque.

Figura 2-4 Ataque de servicio global
Realizado por: Martínez, Carlos, 2015

Denegación de servicio global (atk6-flood_router26 eth0*)*, mediante el envío masivo de paquetes router advertisement, un atacante está en la capacidad de inundar el canal de comunicaciones a la vez que provoca un desbordamiento de buffer en las PCS que reciben el ataque, dado que las solicitudes re router advertisement son enviadas a la dirección de multicast, este ataque será efectivo para todo el segmento de red, ocasionando que las PCS utilicen el 100% de sus recursos de procesador para analizar y adoptar un supuesto nuevo router como Gateway.

Ataque de intercepción de tráfico.

Para este ataque se escribe el número 14, se escribe la interfaz por donde va a lanzar el ataque, en este caso eth0 e inicia el ataque. Primero todo el tráfico será direccionado a la máquina del atacante y automáticamente se levantara un wireshark para poder examinar los paquetes que la red.

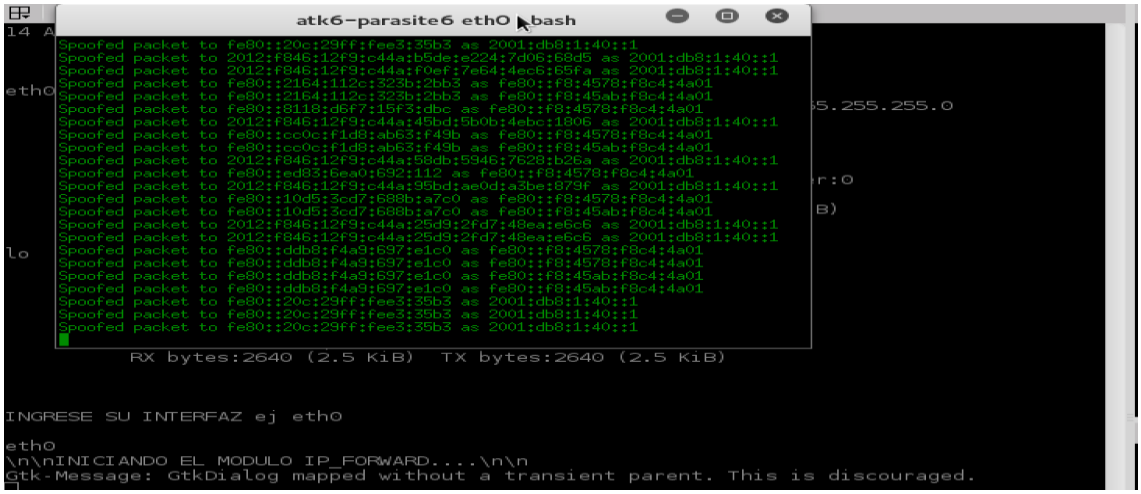


Figura 23-4 Ataque de Intercepción de tráfico
Realizado por: Martínez, Carlos, 2015

Ataques de Intercepción de tráfico (atk6-parasite6 eth0) mediante el envío selecto de solicitudes de router advertisement, es posible suplantar la identidad de los routers de red, con lo cual todas las victimas enviarían el trafico destinado para otras redes a la dirección suplantada por el atacante, de esta manera el atacante estaría en la posibilidad de capturar todo el tráfico proveniente de las victimas así como re-ensamblarlo y reproducirlo, esto para servicios basados en VOIPv6.

Generación de Payloads mediante tunneling IPv6 (msfvenom) mediante la creación de payloads interactivos, un atacante estaría en la capacidad de tomar el control de la víctima utilizando como medio de transmisión en capa 3 IPv6.

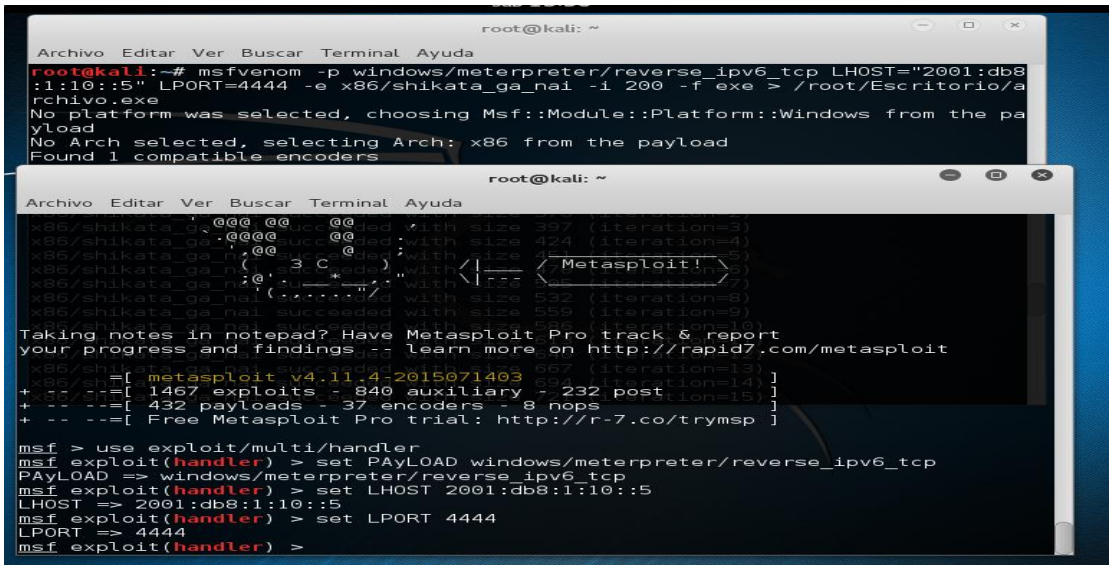


Figura 24-4 Generación de Payloads mediante tunneling
Realizado por: Martínez, Carlos, 2015

Ataques client side (metasploit), mediante la utilización del framework de pentesting Metasploit, un atacante está en la capacidad de simular un servidor web falso, y alojar código malicioso en el contenido de la página por defecto, una vez que la víctima ingrese a la página maliciosa, consumirá el vector de ataque, el cual estará embebido en IPv6 TCP, con lo que se simulará un tráfico aparentemente normal, bypass la protecciónde los dispositivos de seguridad perimetral y el cracker podrá tomar el control de la víctima.

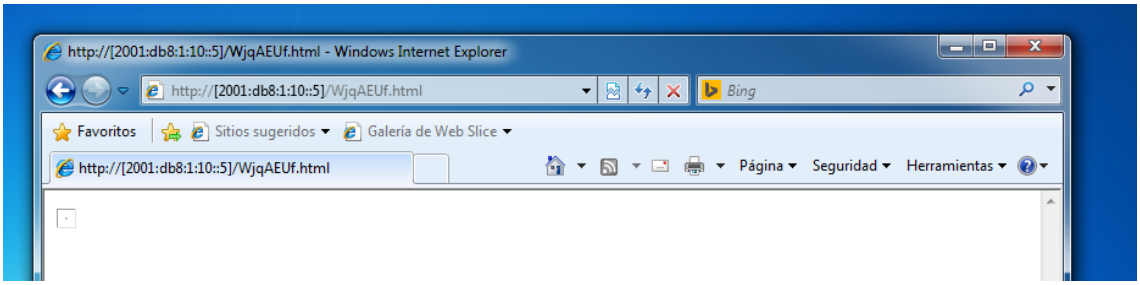


Figura 25-4 Ataques Client Side (Metasploit)
Realizado por: Martínez, Carlos, 2015

4.3Informe de análisis, valoración y posible tratamiento de riesgos sobre las vulnerabilidades encontradas en infraestructuras IPv6.

A continuación se muestra la el informe de las vulnerabilidades encontradas.

Tabla 1-4 Informe de vulnerabilidades

Ataque realizado	Criterio de seguridad afectado	Herramienta utilizada	Descripción	Mitigación	Valoración
Descubrimiento de direcciones locales IPv6 mediante búsqueda en segmentos de red ipv4	Confidencialidad	atk6-alive6 -4 192.168.1.0/24 eth0	Mediante la herramienta alive6 es posible enviar paquetes icmpv6 a la dirección de multicast FF02::1, con lo cual todos los dispositivos que se encuentren habilitados IPv6 responderán al paquete ICMPv6 indicando su dirección global	Debido al funcionamiento de IPv6 mediante el envío de tráfico a direcciones de multicast, al momento no se puede mitigar el ataque	Low

Detección de nuevas direcciones IP	Confidencialidad	atk6-detect-new-ip6 eth0	Por defecto cuando un nuevo host es agregado a la red mediante IPv6, envía solicitudes de neighbor discovery, con lo cual si un atacante inicia un sniffer, es capaz de capturar tanto la nueva dirección de link local así como la dirección de global link, además la herramienta permite adicionar un script que puede ser ejecutado cuando se detecte una nueva dirección que se ha añadido al segmento de red local	Para protegerse ante este ataque se ha definido un mecanismo llamado SEND (Secure Neighbor Discovery) que proporciona seguridad a los mensajes NDP	Low
Detección de servidores de DHCPv6	Confidencialidad	atk6-dump_dhcp6 eth0	La herramienta permite descubrir los servidores de DHCPv6 que se encuentren habilitados en el segmento de red local, lo cual atenta a la confidencialidad de la información, por cuanto un atacante podría generar un ataque de denegación de servicio sobre el servidor DHCP y suplantar la identidad del mismo con parámetros erróneos que le permitirían controlar la asignación de direcciones IP	Debido a que los paquetes Offer de DHCPv6 se envían en texto plano, al momento no es posible mitigar el ataque	Medium
Detección de routers	Confidencialidad	atk6-dump_router6 eth0	Permite detectar los routers conectados en el segmento de red local, lo cual atenta contra la confidencialidad de la información	Para evitar ser víctima de este ataque se recomienda bloquear el descubrimiento de routers en su configuración con <<routerdiscovery=”disabled”	Medium
Escaneo de Puertos	Confidencialidad	nmap -6 2001:db8:1:40::3 --open -O	Mediante la ejecución de Nmap, es posible determinar el estado operativo en el cual se encuentra un puerto respecto al servicio brindado, además es posible determinar el tipo de sistema operativo de la víctima y numero de saltos que debe atravesar el atacante hasta llegar a su objetivo, de esta manera el atacante está en la capacidad de conocer los dispositivos de capa 3 que realizan forwarding de sus paquetes pudiendo inclusive realizar ataques sobre estos routers	A fin de mitigar un posible ataque de escaneo de puertos, se deberá realizar la implementación de listas de control de acceso a nivel de soluciones de filtrado de paquetes en capa 4	Medium

Ataque de Fragmentación de Paquetes	Disponibilidad	atk6-fragmentation6 eth0 2001:db8:1:10::2	Por defecto mediante la utilización de IPv6 los routers y dispositivos de capa 3 no fragmentan los paquetes cundo son enviados desde sus interfaces, sin embargo mediante el uso de la herramienta frag6, es posible crear una fragmentación de los paquetes que son enviados a un host final, mediante esta técnica, el atacante está en la posibilidad de enviar paquetes con distintos tamaños a la víctima, evadiendo medidas de seguridad implementadas en soluciones IDS, cuando la víctima recibe el ataque, necesita agregar recursos de memoria a los buffers creados para la recepción de cada paquete, el incremento en la memoria asignada genera una baja de recursos, lo que atenta a la disponibilidad de la información.	A fin de mitigar un posible ataque de fragmentación, se deberá realizar la implementación de listas de control de acceso a nivel de soluciones de filtrado de paquetes en capa 4	Medium
Ataque ICMPv6 Smurf	Disponibilidad	atk6-smurf6 eth0 2001:db8:1:40::2	Envía solicitudes echo ICMPv6 a todas las direcciones de multicast disponibles, como resultado todos los dispositivos re envían trafico ICMPv6 a la víctima	Debido al funcionamiento de IPv6 mediante el envío de tráfico a direcciones de multicast, al momento no se puede mitigar el ataque	High
Denegación de Servicio hibrido dirigido hacia los routers	Disponibilidad	atk6-denial6 eth0 2001:db8:1:40::21	Genera una gran cantidad de solicitudes icmpv6, route advertisement y neighbor advertisement, lo cual atenta a la disponibilidad de todos los routers que se encuentren en el path hacia la victima	Con las soluciones anteriores sobre estos protocolos es posible mitigar estos ataques.	High
Denegación de Servicio hibrido hacia la victima	Disponibilidad	atk6-denial6 eth0 2001:db8:1:40::22	Genera una gran cantidad de solicitudes icmpv6, route advertisement y neighbor advertisement hacia la víctima del ataque, no afecta a los dispositivos de networking que se encuentran en el path	Con las soluciones anteriores sobre estos protocolos es posible mitigar estos ataques.	High
Explotación de vulnerabilidades en IPv6	Disponibilidad	atk6-exploit6 eth0 2001:db8:1:40::21	Explota la vulnerabilidades CVE-2003-0429 que generaría una denegación de servicio por el envío excesivo de prefijos de red que no se rigen el estándar.	Debido al funcionamiento de IPv6 mediante el envío de tráfico a direcciones de multicast, al momento no se puede mitigar el ataque	Medium

Explotación de vulnerabilidades en IPv6	Disponibilidad	atk6-exploit6 eth0 2001:db8:1:40::2 2	Explota la vulnerabilidad CVE-2004-0257 que generaría una denegación de servicio por el flooding de solicitudes TCP SYN mediante el envío de paquetes fuera del tamaño estándar	Debido al funcionamiento de IPv6 mediante el envío de tráfico a direcciones de multicast, al momento no se puede mitigar el ataque	Medium
Explotación de vulnerabilidades en IPv6	Disponibilidad	atk6-exploit6 eth0 2001:db8:1:40::2 3	Explota la vulnerabilidad CVE-20 que genera una denegación de servicio por el envío excesivo re paquetes router advertisement	Los equipos Cisco disponen de actualizaciones que corrigen esta vulnerabilidad.	Medium
Denegación de servicio global	Disponibilidad	atk6-flood_router26 eth0	Mediante el envío masivo de paquetes router advertisement, un atacante está en la capacidad de inundar el canal de comunicaciones a la vez que provoca un desbordamiento de buffer en las pcs que reciben el ataque. Dado que las solicitudes re router advertisement son enviadas a la dirección de multicast, este ataque será efectivo para todo el segmento de red, ocasionando que las pcs utilicen el 100% de sus recursos de procesador para analizar y adoptar un supuesto nuevo router como Gateway	A fin de evitar una denegación de servicio a nivel global, se deberá realizar la implementación de listas de control de acceso a nivel de soluciones de filtrado de paquetes en capa 4	High
Análisis de Vulnerabilidades	Integridad, Confidencialidad, Disponibilidad	Nessus	El escáner de vulnerabilidades Nessus, permite analizar a la víctima desde el punto de vista de un atacante, con el fin de obtener las vulnerabilidades conocidas que posee la víctima, un posible software para explotar dichas vulnerabilidades y la solución recomendada para la vulnerabilidad encontrada.	Para evitar un escaneo de vulnerabilidades, se deberá realizar la implementación de listas de control de acceso a nivel de soluciones de filtrado de paquetes en capa 4. Además se deberá realizar la implementación de soluciones anti-malware, así como realizar una correcta actualización de los sistemas operativos de los activos de información	High
Generación de Payloads mediante tunneling IPv6	Integridad, Confidencialidad, Disponibilidad	msfvenom	mediante la creación de payloads interactivos, un atacante estaría en la capacidad de tomar el control de la víctima utilizando como medio de transmisión en capa 3 IPv6	A fin de evitar una infección a través de payloads, es necesaria la implementación de soluciones IPS, los cuales detecten y cierren las posibles conexiones de las víctimas con su respectivo CCC. Además se deberá contar con soluciones antimalware, las cuales posean sus firmas de datos actualizadas.	High

Ataques Client Side	Integridad, Confidencialidad, Disponibilidad	Metasploit	Mediante la utilización del framework de pentesting Metasploit, un atacante está en la capacidad de simular un servidor web falso, y alojar código malicioso en el contenido de la página por defecto, una vez que la víctima ingrese a la página maliciosa, consumirá el vector de ataque, el cual estará embebido en IPv6 TCP, con lo que se simulará un tráfico aparentemente normal, bypass la protección de los dispositivos de seguridad perimetral y el cracker podrá tomar el control de la víctima	A fin de evitar una infección a través de payloads, es necesaria la implementación de soluciones IPS, los cuales detecten y cierren las posibles conexiones de las víctimas con su respectivo CCC. Además se deberá contar con soluciones antimalware, las cuales posean sus firmas de datos actualizadas.	High
Ataques de Intercepción de tráfico	Integridad, Confidencialidad, Disponibilidad	atk6-parasite6 eth0	mediante el envío selecto de solicitudes deroutersadvertisement, es posible suplantar la identidad de los routers de red, con lo cual todas las victimas enviarían el trafico destinado para otras redes a la dirección suplantada por el atacante, de esta manera el atacante estaría en la posibilidad de capturar todo el tráfico proveniente de las victimas así como re ensamblarlo y reproducirlo, esto para servicios basados en VOIP	Para evitar este ataque se puede usar el bloquear el descubrimiento de routers especificado en un anterior punto.	High

Realizado por: Martínez, Carlos, 2015

4.4Resultados.

4.4.1 Comprobación de la hipótesis.

¿Es posible corregir la vulnerabilidad de seguridad en las estructuras con direccionamiento IPV6 a través del desarrollo de un Framework?

Para comprobar la hipótesis hemos dado una valoración a las vulnerabilidades encontradas que se muestra en la siguiente **tabla 2-4:**

Tabla 2-4. Valoración de vulnerabilidades

Vulnerabilidades Encontradas	Corregida	No Corregida
Vulnerabilidad 1		1
Vulnerabilidad 2	1	
Vulnerabilidad 3		1

Vulnerabilidad 4	1	
Vulnerabilidad 5	1	
Vulnerabilidad 6	1	
Vulnerabilidad 7		1
Vulnerabilidad 8	1	
Vulnerabilidad 9	1	
Vulnerabilidad 10		1
Vulnerabilidad 11		1
Vulnerabilidad 12	1	
Vulnerabilidad 13	1	
Vulnerabilidad 14	1	
Vulnerabilidad 15	1	
Vulnerabilidad 16	1	
Vulnerabilidad 17	1	
TOTAL	12	5

Realizado por: Martínez, Carlos, 2015

La tabla anterior nos presenta los siguientes resultados:

Tabla 3-4 Resultado de valoración de vulnerabilidades

No corrige	Corregido
29,40%	70.60%

Realizado por: Martínez, Carlos, 2015

)

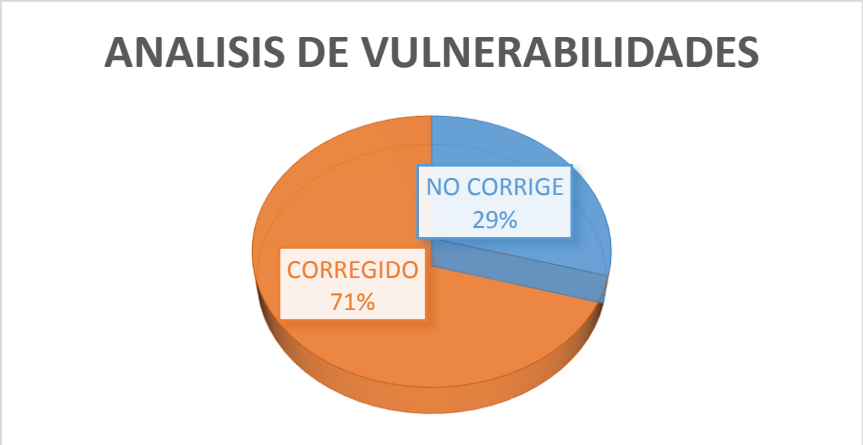


Figura 26-4 Porcentaje del análisis de vulnerabilidades

Realizado por: Martínez, Carlos, 2015

Analisis

Se concluye que la hipotesis se comprueba ya que con la elaboracion de esta metodologia es posible correguir las vulnerabilidades presentes en IPv6. Ademas permite saber a que tipos de ataques pueda ser sometida la infraestructura y por consiguiente da las pautas para relizar una auditoria de seguridad de la informacion mediante el seguimiento de esta metodologia.

CONCLUSIONES

Con los resultados obtenidos se puede concluir lo siguiente:

- Efectivamente el desarrollar un Framework conlleva a un análisis rápido y veras de una infraestructura con direccionamiento IPv6, permitiendo conocer cuáles son las vulnerabilidades existentes en la infraestructura.

- Cuando se hace un análisis de Vulnerabilidades es menester tener una metodología sistemática a seguir para que los resultados de la misma sean óptimos.

- Es importante profundizar el conocimiento en lo que a IPv6 ya que existen vulnerabilidades que a pesar de que su año de aparición fue ya distante del que vivimos, aun no se mitiga esa vulnerabilidad o se difunde un parche de seguridad.

- Se ha concluido que a pesar de encontrar las vulnerabilidades en la infraestructura, algunas en IPv6 al momento no tienen una corrección del error que la causa es decir no pueden ser mitigadas.

RECOMENDACIONES

- Se recomienda para trabajos futuros ampliar el número de vulnerabilidades encontradas, basándose en esta metodología que es exclusivamente para IPv6.
- Se recomienda a los investigadores que busques indagar en la corrección de vulnerabilidades que al momento no se han podido mitigar.
- Cuando se hace un escaneo de vulnerabilidades se debe separa por partes el hardware y software dividiendo en sub grupos, es decir clasificar según la visión del experto de seguridad.
- Si se dispone de una infraestructura con direccionamiento IPv4 se recomienda desactivar IPv6 en los equipos ya que puede ser víctima de ataques infiltrados por vulnerabilidades existentes en este protocolo.

BIBLIOGRAFIA

1. CASTAN SALINAS A. (2007, agosto 15). Análisis activo y pasivo de redes - analisispa.pdf. http://profesores.fi-b.unam.mx/cintia/analisispa.pdf
2. CHOUDHARY A, & SEKELSKY A. (2010). Securing IPv6 network infrastructure: A new security model. En *2010 IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 500-506). http://doi.org/10.1109/THS.2010.5654971
3. COELLAR J, & CEDEÑO J. (2013, febrero 4). *PROPUESTA PARA LA TRANSICIÓN DE IPv4 A IPv6 EN EL ECUADOR A TRAVÉS DE LA SUPERTEL*. Universidad Catolica Santiago de Guayaquil, Guayaquil. Recuperado a partir de http://repositorio.ucsg.edu.ec/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf
4. COELLO M. (2013). *Procedimiento formal de Ethical Hacking para la infraestructura tecnológica de los servicios por internet de la banca ecuatoriana*. Escuela Politecnica Nacional, Quito. Recuperado a partir de http://bibdigital.epn.edu.ec/bitstream/15000/5736/1/CD-4677.pdf
5. DOS SANTOS R, MOREIRA A, ASSENCO REIS E, & SOARES DA ROCHA A. (2010). CUrso IPv6 Básico. Recuperado a partir de http://ipv6.br/media/arquivo/ipv6/file/26/Apostila_Teorica_es.pdf
6. DURDA E, & BULDU A. (2010). IPV4/IPV6 security and threat comparisons. *January 25 2010*, *1*, 7. http://doi.org/10.1016
7. ESPINOSA C, MALDONADO D, VALAREZO C, CARRASCO P, & BARRERA J. (2004). *Implementacion_Practica_Utilizando_IPv6.pdf* (Practico) (p. 84). Quito: Escuela Politecnica del Ejercito del Ecuador. Recuperado a partir de http://www.redesecuador.com/Implementacion_Practica_Utilizando_IPv6.pdf
8. GARCIA MARTIN C. (2012, julio). *Análisis de seguridad en redes IPv6*. Universidad Carlos III de Madrid. Recuperado a partir de http://e-archivo.uc3m.es/handle/10016/16707
9. GEROMETTA O. (2007, octubre 26). Mis Libros de Networking: Introducción a la Conmutación Ethernet y el Enrutamiento IP. Recuperado a partir de http://librosnetworking.blogspot.com/2007/10/introduccin-la-conmutacin-ethernet-y-el.html

10. GERRERO POLICIA CIBERNETICA. (2014). Seguridad Informatica Para Usuarios Finales 01. Recuperado a partir de http://ciberneticagro.blogspot.com/2014/08/seguridad-informatica-para-usuarios.html
11. GHEBREGZIABHER T, PUTTONEN J, HAMALAINEN T, & VIINIKAINEN A. (2006). Security analysis of flow-based fast handover method for mobile IPv6 networks. En *20th International Conference on Advanced Information Networking and Applications, 2006. AINA 2006* (Vol. 2, p. 5 pp.-). http://doi.org/10.1109/AINA.2006.299
12. HORLEY E. (2014). Practical IPv6 for Windows Administrators - (p. 250). NEW YORK: Steve Anglin, Mark Beckner, Ewan Buckingham, Gary Cornell, Louise Corrigan, James T. DeWolf, Jonathan Gennick, Jonathan Hassell, Robert Hutchinson, Michelle Lowman, James Markham, Matthew Moodie, Jeff Olson, Jeffrey Pepper, Douglas Pundick, Ben Renow-Clarke, Dominic Shakeshaft, Gwenan Spearing, Matt Wade, Steve Weiss. Recuperado a partir de https://books.google.es/books?hl=es&lr=&id=m5N0AgAAQBAJ&oi=fnd&pg=PP3&dq=edward+horley+practical+ipv6+for+windows+administrators+&ots=DMR9SGZdoN&sig=IrQQtx9lbyZT85XYMYaAilJQcYQ#v=onepage&q=edward%20horley%20practical%20ipv6%20for%20windows%20administrators&f=false
13. ISECOM - Institute for Security and Open Methodologies. (s. f.). Recuperado 17 de junio de 2015, a partir de http://www.isecom.org/
14. JAIMES SANTOS L, & BAUTISTA W. (2007). IPV6 en la universidad de pamplona: estado del arte. *Scientia et Technica*, *1*(37), 415.
15. LA FLECHA DIARIO DE CIENCIA Y TECNOLOGIA. (2008, mayo 8). Los 10 principales errores de seguridad TI que cometen los departamentos informÃ¡ticos en las Pymes. Recuperado 25 de agosto de 2015, a partir de http://laflecha.net/archivo/canales/seguridad/noticias/los-10-principales-errores-de-seguridad-ti-que-cometen-los-departamentos-informaticos-en-las-pymes
16. LÓPEZ J. (2014). *FACTIBILIDAD DE IP SEC PARA IPV6 EN LA RED DE LA UNIVERSIDAD POLITÉ CNICA SALESIANA, SEDE QUITO*. ESPE, Quito. Recuperado a partir de http://repositorio.espe.edu.ec/bitstream/21000/9081/1/T-ESPE-048317.pdf
17. MIERES J. (2009). Ataques informaticos, 17.

18. PALET J. (1999). Tutorial de IPv6.pdf. Recuperado 26 de agosto de 2015, a partir de http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf
19. HERZOG PETE. (2003, agosto 23). OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad. ISECOM.
20. ROBLES M. (2008). *«QoS en redes wireless con IPv6»* (Maestria). Universidad Nacional de La Plata, Argentina. Recuperado a partir de http://sedici.unlp.edu.ar/bitstream/handle/10915/4149/Documento_completo.pdf?sequence=1
21. BUSTAMANTE SANCHEZ R. (2005). *Seguridad en redes* (tesis). Universidad Autonoma de Hidalgo. Recuperado a partir de http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf
22. SAENZ GONZALEZ G. (2009, agosto). *DISENO DE UN LABORATORIO DE ANALISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACION EN REDES DE COMPUTO* (tesis). escuela Superior de Ingenieria Mecanica y electrica, Instituto Politecnico Nacional, Mexico. Recuperado a partir de http://tesis.ipn.mx:8080/xmlui/handle/123456789/8340
23. *Seguridad Informatica*. (2002, junio 26). Universidad Tecnologia Nacional. Recuperado a partir de http://www.segu-info.com.ar/tesis/
24. SILES PELAEZ R. (2002, junio). *(Analisis de seguridad de la familia de de protocolos TCP-ip y sus servicios asociados* . (maestria). Recuperado a partir de http://ftp.nluug.nl/ftp/pub/os/Linux/doc/LuCaS/Manuales-LuCAS/doc-seguridad-tcpip/Seguridad_en_TCP-IP_Ed1.pdf
25. THOMSON BELLCORE S, & NARTEN T. (1998). IPv6 Stateless Address Autoconfiguration. Recuperado 22 de julio de 2015, a partir de https://www.google.es/search?hl=es&q=THOMSON+S,+%E2%80%9CNetwork+Working+Group%E2%80%9D,+Bellcore+Standards+Track,+IBM+Diciembre+1998
26. VALDEZ ALVARADO A. (2013). OSSTMM 3. *Revista de Información, Tecnología y Sociedad*. Recuperado a partir de http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100013&script=sci_arttext&tlng=es

27. VAZQUEZ AMENDARIZ W. (2005, abril). *METODOLOGIA DE MIGRACION DE REDES IPV4 A IPV6 Caso Práctico : ESPE LATACUNGA*. ESPE, Latacunga. Recuperado a partir de http://repositorio.espe.edu.ec/bitstream/21000/4160/1/T-ESPEL-0011.pdf
28. VERDEJO ALVAREZ G. (2009). Encabezado IPv6 « IP reference. Recuperado 3 de agosto de 2015, a partir de https://ipref.wordpress.com/2009/02/20/ipv6-header/
29. VILLALON HUERTA A. (2010). *Seguri dad en Unix y redes.* (Vol. 2). Cataluyna. Recuperado a partir de https://www.google.com.ec/?gfe_rd=cr&ei=sYtcVfD7C5Cw8wev_4Ao&gws_rd=ssl#q=HUERTA%2C+Antonio+Villal%C3%B3n.+Seguri+dad+en+Unix+y+redes.+(Versi%C3%B3n+2.1)+
30. WANG YI D, FAN JIAN B, PAM PUI C, & LAM D. (2008). The cytotoxic and stress responses of human trabecular meshwork cells treated with triamcinolone acetonide. *Molecular Vision*, *14*, 105-113.

ANEXOS

Anexo A. . SCRIPT PARA ANALISIS DE VULNERABILIDADES EN IPv6

```
shc -v -f tesis_carlos
#endif

static  char data [] =
#define     inlo_z      3
#define     inlo        ((&data[0]))
        "\030\122\324"
#define     chk1_z      22
#define     chk1        ((&data[4]))
        "\070\376\104\142\223\227\340\135\064\115\157\125\224\017\171\131"
        "\151\242\252\147\347\120\175\245\333\337\322"
#define     tst2_z      19
#define     tst2        ((&data[30]))
        "\222\044\247\344\273\332\076\121\113\274\115\172\142\065\154\011"
        "\352\035\033\331\074"
#define     msg2_z      19
#define     msg2        ((&data[53]))
        "\216\121\342\010\021\141\110\166\213\040\307\041\120\326\377\354"
        "\217\142\062\054\050\370\057"
#define     xecc_z      15
#define     xecc        ((&data[77]))
        "\223\205\222\371\053\131\327\032\310\167\041\302\135\227\006\100"
        "\324\371\067\015\331"
#define     shll_z      10
#define     shll        ((&data[95]))
        "\323\050\346\171\145\164\172\311\026\325\227"
#define     chk2_z      19
#define     chk2        ((&data[109]))
        "\313\202\017\156\164\361\013\311\127\122\067\005\261\240\147\075"
        "\071\355\115\120\167\205\270"
```

```
#define     rlax_z      1
#define     rlax        ((&data[129]))
        "\306"
#define     text_z      5522
#define     text        ((&data[427]))
        "\075\305\162\065\364\304\035\351\127\243\173\217\260\125\322\347"
        "\300\151\327\143\246\243\345\266\133\173\125\354\115\214\016\212"
        "\122\201\277\107\105\335\060\235\200\253\054\060\001\376\030\302"
        "\150\360\046\017\223\014\306\356\207\033\333\325\250\352\140\372"
        "\153\040\101\261\375\161\117\175\035\173\256\037\172\306\341\343"
        "\266\010\362\112\024\270\071\234\324\025\161\174\377\321\166\153"
        "\361\270\035\356\051\154\154\107\347\032\146\142\341\110\105\230"
        "\120\070\342\145\360\033\001\304\060\163\100\060\104\267\233\066"
        "\157\271\045\231\045\221\340\015\253\107\157\215\217\265\045\340"
        "\355\007\105\335\043\106\242\124\271\343\204\376\232\040\064\012"
        "\331\132\243\377\353\204\014\227\313\174\044\133\061\111\073\036"
        "\121\201\374\165\307\237\311\201\202\116\200\035\157\265\050\111"
        "\017\314\110\372\120\124\222\034\321\266\167\002\000\262\041\122"
        "\063\036\307\373\275\220\175\100\337\375\135\116\263\205\227\302"
        "\121\340\275\242\065\117\276\006\006\065\010\007\350\052\131\034"
        "\110\041\030\005\262\225\105\221\223\243\340\106\051\167\011\173"
        "\130\306\035\215\026\334\223\034\022\234\044\372\306\175\027\017"
        "\236\057\025\120\304\133\342\130\376\302\236\050\072\247\243\222"
        "\156\301\040\204\235\263\241\260\120\276\213\105\323\370\353\015"
        "\230\040\213\301\250\107\341\044\167\225\270\112\057\171\372\351"
        "\046\337\217\306\354\137\134\123\071\265\364\176\355\236\323\032"
        "\115\113\364\002\047\364\161\272\160\005\033\226\366\030\266\062"
        "\337\040\316\326\005\152\202\005\160\247\211\357\364\037\156\047"
        "\343\332\052\102\131\161\007\100\250\333\153\020\122\073\356\240"
        "\175\213\027\134\320\331\027\036\112\132\131\040\306\130\151\102"
        "\257\042\265\310\124\035\161\150\170\324\312\054\127\042\015\234"
        "\103\365\165\252\040\347\071\301\031\000\117\335\152\024\076\311"
        "\337\216\005\176\311\017\006\203\223\146\347\126\120\110\036\320"
```

"\116\042\157\331\045\134\155\154\367\121\374\127\323\321\142\312"
"\106\331\327\115\037\132\234\343\333\307\104\067\342\366\341\034"
"\013\025\203\253\133\305\263\167\334\331\350\034\106\063\362\152"
"\367\033\115\112\251\131\151\207\373\137\342\231\221\047\353\155"
"\236\322\105\016\373\144\010\005\001\026\115\321\012\107\310\232"
"\174\330\356\261\352\243\240\344\341\367\017\360\062\355\207\016"
"\334\064\331\347\173\161\114\016\120\124\166\023\347\031\342\223"
"\120\324\356\315\002\227\323\367\377\242\056\144\202\355\362\247"
"\153\251\305\062\342\376\121\037\366\057\237\330\255\164\217\077"
"\264\222\052\174\010\173\323\027\377\133\165\176\255\165\063\355"
"\244\115\023\251\017\251\052\005\164\370\251\140\107\175\166\017"
"\371\241\215\026\357\331\366\236\064\143\102\064\142\045\322\320"
"\170\006\356\106\156\206\042\011\025\350\252\317\276\120\160\200"
"\230\327\022\317\255\217\112\173\012\064\257\042\315\121\362\006"
"\047\002\320\222\227\142\371\052\274\177\356\243\365\176\326\073"
"\047\061\367\175\036\166\346\162\140\243\065\306\255\123\102\007"
"\120\372\341\223\234\207\231\064\202\034\044\241\362\016\217\222"
"\256\353\056\066\144\245\304\160\016\053\175\056\172\327\331\217"
"\314\052\340\046\277\317\034\222\304\021\141\022\356\115\063\106"
"\153\236\077\072\034\047\162\167\150\301\203\316\122\047\144\306"
"\230\157\203\061\272\347\320\212\351\167\356\273\123\261\162\375"
"\323\333\216\261\054\036\100\312\172\367\267\022\310\315\144\073"
"\211\230\033\371\072\077\114\372\351\055\104\313\072\140\242\333"
"\053\003\075\122\271\163\307\340\057\333\311\150\102\332\156\250"
"\305\014\102\147\322\303\372\142\033\264\124\314\100\351\164\257"
"\042\240\311\141\173\032\171\351\373\156\276\100\227\000\102\364"
"\227\220\154\372\250\006\316\050\117\365\364\234\354\325\103\255"
"\327\047\343\220\133\242\107\273\232\271\307\361\034\034\270\260"
"\357\363\072\044\151\172\274\356\043\342\201\330\003\176\160\307"
"\123\276\154\026\076\277\261\267\131\143\132\267\262\114\053\017"
"\105\073\024\140\146\332\266\310\357\042\377\113\341\147\242\151"
"\026\026\330\227\032\376\140\101\155\250\235\130\122\136\264\272"
"\111\365\342\275\111\242\260\133\165\364\105\054\146\342\244\047"

"\365\020\150\146\322\021\143\215\201\230\052\377\123\162\110\165"
"\025\312\241\053\224\250\056\102\053\220\177\364\047\275\223\270"
"\375\044\152\173\127\230\032\147\051\034\345\106\342\110\076\365"
"\163\027\315\374\167\305\042\351\360\252\203\316\123\047\316\277"
"\371\105\144\012\055\165\261\172\035\205\024\365\360\267\146\274"
"\326\144\124\215\057\076\312\142\263\142\207\162\034\120\126\116"
"\125\254\117\023\166\235\177\102\105\177\230\227\342\241\250\105"
"\334\040\341\136\144\217\223\041\337\223\224\174\211\253\245\330"
"\012\046\261\352\344\366\202\227\355\322\215\236\276\205\171\174"
"\244\055\244\300\217\046\340\162\175\351\263\350\127\304\332\312"
"\052\333\256\253\247\006\264\027\261\301\207\350\205\011\262\035"
"\102\214\221\112\037\274\363\206\340\073\113\362\157\173\045\315"
"\167\336\114\314\036\107\111\267\030\020\247\207\303\112\367\146"
"\371\071\152\203\363\140\273\215\151\361\322\365\056\224\206\116"
"\142\223\175\372\111\255\261\337\323\304\001\143\133\367\044\167"
"\157\075\301\205\126\232\333\012\251\014\203\342\346\323\041\201"
"\322\202\221\242\067\356\262\132\367\254\135\103\014\076\206\034"
"\340\050\227\322\200\214\045\133\020\264\301\131\120\267\047\055"
"\052\064\221\127\072\000\200\014\325\176\225\206\261\323\234\130"
"\131\377\076\026\016\045\003\071\227\362\024\265\116\121\113\005"
"\364\040\040\045\101\073\141\031\330\365\120\037\351\362\177\261"
"\000\027\224\010\333\025\103\343\216\110\356\373\100\030\315\237"
"\337\060\347\164\225\131\261\120\023\073\046\374\245\202\106\033"
"\363\163\102\102\305\011\076\314\331\217\042\000\357\214\242\175"
"\063\334\235\001\352\164\124\350\317\006\256\203\144\242\125\304"
"\025\345\377\207\334\145\146\030\066\347\170\376\042\152\254\054"
"\345\303\247\044\333\265\370\263\275\235\247\123\206\342\212\142"
"\307\267\047\173\302\317\251\020\165\173\212\045\345\305\060\104"
"\231\064\253\053\003\223\346\026\222\024\157\147\010\000\114\356"
"\323\076\311\067\254\163\247\070\302\135\037\323\056\064\124\330"
"\020\171\113\367\050\146\375\136\260\020\052\330\324\106\207\157"
"\174\167\066\365\006\115\027\227\157\145\104\350\365\316\112\034"
"\211\055\062\163\342\256\004\265\063\062\351\144\102\327\022\006"

"\301\224\007\144\246\205\261\000\206\042\211\373\332\336\375\373"
"\305\035\152\344\310\031\237\106\235\341\214\216\237\222\214\072"
"\265\064\254\273\256\331\022\257\043\040\267\172\274\207\160\325"
"\064\277\200\212\201\034\324\012\000\265\342\056\047\213\100\215"
"\161\171\374\047\332\020\243\114\372\074\044\235\217\254\332\353"
"\071\136\015\353\173\032\105\375\161\327\164\057\043\247\030\342"
"\201\131\274\344\322\173\172\231\240\236\007\272\251\144\227\355"
"\356\131\111\217\140\316\100\203\376\307\116\370\074\140\050\051"
"\071\103\035\351\263\020\116\206\060\003\261\074\034\105\004\155"
"\030\234\252\276\276\266\337\304\156\355\354\114\226\162\012\040"
"\350\266\301\214\227\166\367\364\174\237\364\276\350\312\314\052"
"\341\247\365\141\020\321\203\044\020\135\237\127\270\313\131\315"
"\141\221\115\147\203\107\131\010\000\254\033\175\126\177\362\024"
"\332\023\220\172\210\161\110\123\310\031\167\026\276\356\110\136"
"\223\200\236\066\177\373\315\236\275\055\131\015\040\043\177\005"
"\056\356\154\157\316\212\213\205\217\057\075\257\003\327\123\065"
"\342\264\031\116\262\357\277\031\343\316\007\130\355\043\001\273"
"\235\035\313\132\352\041\250\324\153\374\066\214\347\052\330\370"
"\224\117\161\370\167\266\205\030\102\132\371\006\205\377\171\122"
"\201\175\376\257\101\225\007\161\060\346\135\276\053\175\314\224"
"\310\375\237\045\212\317\033\001\072\374\162\150\334\261\022\050"
"\342\242\240\115\275\076\254\364\256\372\376\166\234\341\122\106"
"\123\100\132\152\116\353\047\116\247\353\154\155\334\060\001\346"
"\206\061\054\260\237\323\233\300\334\261\226\250\255\301\250\066"
"\273\026\035\067\015\176\144\330\033\072\376\367\005\144\336\250"
"\271\330\060\147\262\146\220\145\334\302\341\355\110\060\306\055"
"\022\201\137\041\254\255\105\025\025\077\214\101\105\143\323\366"
"\273\207\375\162\020\132\364\057\103\330\045\327\124\144\241\036"
"\322\262\114\254\355\225\133\114\060\150\375\257\121\021\336\027"
"\253\177\367\035\136\322\133\047\273\114\031\167\203\170\176\145"
"\073\254\265\374\216\156\321\045\231\272\056\006\212\200\117\307"
"\237\271\273\155\144\252\003\141\247\210\333\335\335\334\340\047"
"\154\331\205\370\226\176\127\227\222\141\136\153\325\020\003\002"

"\076\320\150\256\377\066\033\020\127\345\206\014\336\363\125\173"
"\012\235\351\173\006\100\111\350\165\350\056\110\114\273\201\347"
"\114\020\006\342\366\331\374\117\076\364\103\303\143\021\326\272"
"\175\145\366\206\115\263\372\263\353\065\367\247\071\373\355\201"
"\336\077\067\334\255\241\365\316\002\346\012\026\174\255\340\220"
"\353\172\321\042\300\251\225\213\171\307\356\001\056\327\034\376"
"\016\160\266\140\367\115\375\142\241\147\240\263\266\313\147\320"
"\322\131\013\011\111\253\166\045\272\307\153\235\065\132\347\266"
"\050\103\153\333\172\153\305\342\262\244\315\134\234\332\337\056"
"\357\166\136\276\036\320\153\264\262\042\111\376\017\351\322\300"
"\144\305\011\163\375\360\243\172\054\326\046\254\117\307\024\313"
"\027\043\340\342\325\165\203\274\373\215\344\052\030\043\141\161"
"\037\101\115\047\351\044\113\221\350\165\375\030\103\120\205\063"
"\125\143\354\061\360\125\075\347\231\056\327\133\267\046\176\202"
"\331\047\012\366\334\242\050\057\003\203\136\127\040\316\325\125"
"\103\371\335\062\145\122\213\375\377\317\227\045\271\345\316\034"
"\104\206\337\226\112\167\065\272\313\154\373\101\302\344\304\337"
"\325\077\007\065\272\102\216\160\012\267\345\262\046\210\365\113"
"\072\253\225\374\153\175\372\275\227\254\027\206\114\121\363\043"
"\203\070\201\134\174\214\254\216\170\214\144\234\175\307\256\335"
"\234\104\251\014\026\257\146\177\323\013\300\250\340\232\357\071"
"\246\070\244\276\155\114\122\061\064\250\005\236\233\265\234\274"
"\330\266\343\000\040\125\235\271\173\243\057\350\356\162\374\013"
"\214\110\023\236\021\235\157\006\307\212\125\056\142\041\246\241"
"\074\053\113\235\156\317\333\003\076\007\233\372\030\150\076\026"
"\044\112\035\006\353\320\253\174\140\351\316\112\100\305\022\105"
"\363\270\047\103\161\045\217\034\106\232\251\261\302\220\052\016"
"\043\322\045\212\065\350\105\130\263\225\352\070\201\002\107\236"
"\066\355\375\147\076\071\302\136\042\152\014\007\153\300\111\031"
"\320\333\060\316\243\020\023\235\316\127\075\222\267\036\302\041"
"\055\336\003\053\215\276\316\273\354\247\373\166\015\363\207\014"
"\263\254\231\013\004\110\112\067\072\315\036\074\341\217\377\201"
"\236\047\342\210\364\115\074\234\237\274\123\145\064\101\202\050"

"\022\104\105\150\375\161\110\240\352\134\130\221\060\051\107\022"
"\104\352\035\112\146\032\131\036\041\003\270\227\206\047\367\277"
"\327\324\243\336\037\134\247\202\052\064\337\163\324\277\347\353"
"\261\127\354\242\223\064\063\355\144\162\115\226\336\136\021\035"
"\044\257\347\051\267\003\236\075\262\247\230\011\326\065\214\137"
"\156\267\175\354\273\102\054\253\164\372\350\051\077\210\061\233"
"\351\363\210\277\012\363\237\366\223\000\071\130\132\250\106\353"
"\161\327\024\110\315\041\070\270\101\226\254\130\055\334\014\164"
"\174\207\365\311\373\115\037\374\077\227\004\240\025\202\160\375"
"\330\365\261\353\307\165\175\000\136\252\161\065\016\265\140\176"
"\261\107\155\132\006\167\336\066\114\167\201\237\337\154\076\163"
"\271\350\064\347\123\247\153\043\257\366\325\061\176\212\354\002"
"\150\360\364\163\016\277\254\112\010\202\132\303\147\171\166\001"
"\306\147\340\176\335\177\026\243\377\014\027\317\044\354\227\051"
"\233\171\263\202\162\242\310\176\206\054\103\142\173\163\052\252"
"\231\221\242\201\330\325\077\124\300\323\320\341\106\314\057\147"
"\042\340\327\011\026\062\300\010\214\033\262\352\177\024\274\133"
"\211\310\061\203\312\066\030\163\307\156\050\320\003\164\336\064"
"\336\373\057\240\233\067\340\247\263\116\177\213\155\154\142\354"
"\355\062\105\021\004\012\346\106\350\270\324\271\175\334\353\076"
"\113\274\107\246\013\034\306\042\314\060\372\372\105\374\107\067"
"\376\002\022\101\230\010\045\034\151\356\100\064\137\363\243\316"
"\166\141\153\317\351\136\312\357\312\102\220\160\045\135\146\016"
"\343\043\112\027\315\365\130\117\252\055\023\152\102\263\007\374"
"\263\160\037\001\274\034\325\006\157\261\002\051\155\171\303\244"
"\364\217\117\036\307\206\000\323\166\250\142\304\305\257\356\362"
"\220\327\167\252\103\340\017\275\064\116\133\035\054\026\210\005"
"\372\124\376\267\023\252\241\202\175\262\114\301\065\242\253\200"
"\344\133\014\255\156\172\263\160\333\366\277\214\071\032\320\212"
"\123\211\312\372\022\341\211\153\226\341\012\070\277\136\265\077"
"\250\004\043\247\022\336\164\112\274\104\121\201\065\277\176\105"
"\176\170\333\325\054\304\155\313\367\235\000\154\147\362\245\230"
"\067\324\126\357\222\311\133\006\167\273\241\062\043\247\263\253"

"\220\025\373\335\147\073\011\111\342\324\036\246\371\372\376\171"
"\012\067\220\067\167\253\263\033\074\222\022\254\176\126\041\351"
"\370\002\136\011\157\163\317\257\024\255\301\076\050\254\234\340"
"\301\327\115\354\121\322\302\246\150\354\012\254\111\204\055\340"
"\336\133\372\131\007\277\234\112\144\034\274\125\057\135\223\334"
"\120\352\203\016\144\335\301\277\153\256\205\310\317\117\325\151"
"\140\251\333\066\363\363\274\300\066\272\276\256\042\200\341\202"
"\134\177\266\262\254\366\354\257\075\251\116\016\321\070\010\051"
"\343\317\371\333\145\153\162\222\351\021\335\347\173\100\041\033"
"\212\131\314\160\077\124\132\323\132\042\350\006\064\033\245\024"
"\057\312\104\271\003\015\243\124\312\072\345\051\213\174\111\103"
"\361\063\204\012\230\162\137\171\244\004\304\023\357\305\063\364"
"\011\226\026\205\101\346\012\203\010\253\314\105\034\146\332\214"
"\214\067\307\144\230\105\050\126\014\027\345\320\277\341\001\245"
"\252\343\300\146\026\336\006\151\235\216\117\351\016\124\171\205"
"\274\045\204\035\034\045\320\022\222\336\222\275\037\342\207\004"
"\171\023\016\367\360\053\115\011\060\112\242\355\114\357\232\123"
"\264\036\211\112\034\256\120\011\111\000\343\022\222\277\201\066"
"\307\227\325\155\254\051\131\310\060\171\077\067\123\112\115\232"
"\261\366\235\167\334\134\002\335\374\321\222\261\133\040\164\060"
"\136\240\130\356\142\052\014\034\255\330\070\254\107\151\153\262"
"\332\314\134\005\246\121\126\130\064\154\003\264\375\026\104\260"
"\354\364\216\361\041\106\305\001\061\302\165\107\357\017\204\311"
"\362\357\106\276\224\242\333\057\305\312\131\104\254\313\020\023"
"\051\155\020\224\130\001\220\246\161\011\351\170\217\071\044\362"
"\324\274\026\062\065\167\007\127\317\212\352\320\162\266\270\172"
"\011\372\112\075\065\062\053\161\172\114\164\150\067\151\364\011"
"\362\005\037\050\230\040\371\035\224\022\042\214\237\270\336\241"
"\133\150\311\116\360\316\353\151\027\033\163\040\113\263\170\373"
"\020\076\200\264\147\131\026\120\027\363\202\344\233\232\073\312"
"\174\076\102\006\377\157\041\214\004\237\275\057\075\111\013\342"
"\315\222\141\131\101\177\317\232\241\314\041\316\201\321\017\121"
"\366\231\052\347\175\236\113\356\043\067\247\240\300\123\303\015"

"\070\101\012\366\350\173\276\110\275\313\104\257\156\260\041\340"
"\235\305\144\141\203\307\216\263\246\360\175\075\205\101\036\273"
"\347\332\220\220\060\213\356\304\044\377\074\316\373\032\327\327"
"\352\144\231\366\013\117\371\121\357\131\220\376\153\217\221\024"
"\047\051\054\256\172\373\044\356\164\017\205\336\105\345\011\323"
"\223\135\233\326\172\076\360\155\047\067\031\323\032\121\167\113"
"\117\240\001\037\152\164\253\237\307\150\220\073\375\231\202\014"
"\007\145\357\251\353\051\304\376\076\106\122\303\221\262\140\175"
"\154\032\361\000\346\332\062\340\064\237\106\104\234\216\257\234"
"\260\203\267\142\052\327\362\331\052\045\247\021\373\001\071\146"
"\042\106\366\071\342\272\116\353\026\211\326\015\153\212\036\156"
"\322\267\105\045\220\215\223\001\031\040\105\327\360\376\172\334"
"\072\142\124\045\202\112\314\244\346\354\044\165\101\046\334\257"
"\321\157\362\211\326\211\146\124\320\176\335\227\222\167\246\206"
"\225\070\127\237\147\305\104\166\124\316\325\217\103\003\077\116"
"\221\235\110\242\066\312\045\106\317\150\332\062\164\264\217\024"
"\334\350\204\031\222\012\147\115\006\144\317\306\100\215\140\332"
"\314\073\017\110\147\271\006\213\201\004\263\205\074\337\276\230"
"\024\025\062\105\320\205\244\146\170\061\145\016\221\272\052\005"
"\311\234\100\010\375\126\167\121\224\107\062\233\341\325\263\320"
"\224\260\061\371\373\140\123\300\234\323\257\175\115\025\275\150"
"\256\377\375\067\323\270\013\323\244\207\367\206\320\011\174\256"
"\310\210\140\204\044\056\256\146\172\211\325\154\156\236\236\052"
"\042\170\317\300\205\134\050\235\327\206\274\267\207\004\135\037"
"\061\010\032\214\345\165\167\201\071\045\234\017\013\250\266\247"
"\217\211\235\350\137\123\237\304\363\334\354\204\250\340\271\022"
"\323\341\374\071\067\367\365\375\363\045\117\075\327\073\070\270"
"\363\070\011\057\127\026\123\235\215\227\157\034\266\150\102\266"
"\031\162\167\245\072\341\212\002\330\311\030\151\304\371\312\117"
"\355\226\220\006\122\063\357\254\125\171\131\030\034\025\143\221"
"\375\276\060\301\113\110\025\365\140\202\244\162\207\051\260\275"
"\054\077\064\320\114\141\132\070\134\245\356\172\162\065\047\004"
"\331\243\310\335\170\151\152\005\275\174\005\147\360\115\061\323"

"\051\355\132\172\027\136\166\025\061\371\117\064\053\334\315\025"
"\005\104\055\313\251\307\146\024\075\211\124\324\011\314\121\170"
"\143\105\157\130\224\223\342\352\173\216\315\175\020\053\331\265"
"\203\011\217\221\344\164\162\216\067\373\225\127\254\316\124\136"
"\171\344\030\001\030\006\123\300\266\306\156\003\215\062\165\144"
"\035\003\315\104\173\011\337\056\202\214\166\377\072\316\362\041"
"\000\026\161\354\104\257\303\211\206\231\271\344\243\105\075\145"
"\124\330\221\244\245\243\343\141\214\221\216\026\240\123\366\355"
"\002\016\042\327\026\121\316\212\210\362\343\045\060\232\071\041"
"\304\232\236\016\101\202\250\154\164\027\302\157\134\163\165\363"
"\204\332\362\073\335\223\077\230\203\160\305\145\126\120\011\100"
"\055\157\072\005\114\065\164\045\362\262\206\314\366\212\253\351"
"\214\057\375\067\104\230\135\177\340\062\276\210\274\165\317\146"
"\054\047\011\236\335\007\313\257\252\331\075\270\123\233\131\367"
"\311\021\023\132\002\326\052\372\134\255\004\343\116\334\360\005"
"\004\221\032\002\331\014\254\123\232\241\175\154\320\220\373\344"
"\131\334\066\201\131\066\052\325\172\045\226\330\014\102\304\373"
"\130\236\067\053\133\061\251\162\343\217\243\345\064\320\067\052"
"\232\023\174\167\025\001\045\005\075\307\137\157\331\121\235\225"
"\151\127\023\322\242\005\311\161\135\245\202\216\117\152\356\033"
"\143\271\235\254\130\020\126\356\330\111\016\102\172\304\163\102"
"\203\136\360\217\015\336\260\150\075\047\011\227\017\017\202\335"
"\104\055\131\373\041\163\347\133\241\272\240\202\042\105\074\151"
"\210\242\055\305\125\177\277\117\373\156\341\056\106\377\230\110"
"\014\123\263\371\147\066\225\377\254\070\124\130\314\224\347\073"
"\304\345\067\307\231\144\355\027\040\210\361\144\326\164\154\325"
"\067\232\167\122\233\272\141\167\260\140\110\376\161\026\107\063"
"\004\060\351\252\266\224\121\033\037\230\243\101\041\264\235\264"
"\351\334\114\026\113\345\175\064\035\142\152\070\162\167\046\042"
"\277\103\056\257\001\253\301\140\362\300\273\044\067\223\166\316"
"\324\365\024\302\217\137\364\206\002\202\150\304\371\110\145\076"
"\121\375\004\275\102\072\340\003\261\050\025\271\371\225\035\144"
"\120\067\043\043\125\064\120\305\313\070\274\141\213\277\107\120"

"\261\373\124\346\325\034\145\351\176\301\176\223\230\110\115\012"
"\371\043\147\301\170\243\025\333\356\104\220\113\043\245\212\125"
"\027\123\274\244\312\152\237\265\353\364\321\161\200\233\331\210"
"\343\255\216\134\327\243\334\220\072\305\030\370\151\051\046\222"
"\067\051\044\370\311\033\101\252\021\171\341\035\022\000\316\160"
"\273\100\377\355\173\214\230\335\127\033\372\070\357\037\202\111"
"\250\372\236\102\073\272\277\357\074\126\163\202\100\213\050\252"
"\072\311\256\304\035\005\203\271\213\264\365\300\325\303\362\204"
"\356\254\222\314\306\237\024\241\146\366\102\177\253\022\051\053"
"\063\317\360\121\044\224\033\070\205\203\350\314\357\254\130\150"
"\327\125\025\211\015\345\363\266\335\072\230\324\057\154\046\131"
"\325\303\167\033\332\155\260\160\022\145\254\013\254\141\222\325"
"\120\150\006\247\137\261\260\036\211\027\326\147\041\033\350\207"
"\073\224\317\331\227\174\156\175\327\130\131\135\046\171\032\156"
"\101\152\126\237\103\366\306\226\000\256\051\035\046\205\034\363"
"\157\007\141\323\145\307\035\105\115\146\215\060\355\022\201\115"
"\257\127\155\267\203\054\261\316\312\233\324\273\370\160\015\227"
"\147\142\232\204\103\222\043\011\050\020\310\061\264\252\330\253"
"\346\144\162\220\347\245\253\354\150\343\146\004\335\253\210\111"
"\342\204\153\104\331\124\010\324\316\357\136\335\250\342\376\214"
"\170\343\341\310\020\066\262\071\171\113\113\166\132\320\034\277"
"\034\144\234\352\314\166\127\011\145\265\113\116\351\013\137\357"
"\137\136\120\206\045\371\277\034\220\201\047\222\273\315\032\046"
"\074\127\371\353\027\274\111\010\241\136\201\015\166\123\231\215"
"\337\225\015\230\376\116\323\253\377\012\056\262\025\142\333\350"
"\302\012\063\361\222\145\001\267\243\317\057\244\152\003\323\327"
"\047\324\002\030\154\276\202\356\246\365\276\207\031\004\256\253"
"\324\171\273\375\315\047\030\100\143\237\267\303\054\141\265\322"
"\332\231\207\030\342\266\075\157\154\057\126\354\343\247\355\204"
"\027\357\123\162\260\244\255\335\045\142\256\362\244\133\351\272"
"\300\251\125\004\167\105\005\204\103\144\042\012\222\112\025\045"
"\357\032\217\357\114\162\330\362\165\230\165\356\045\006\263\075"
"\141\321\374\322\003\030\112\131\322\012\007\374\156\250\010\052"

"\376\273\170\346\271\033\371\125\067\016\331\264\104\226\242\000"
"\161\063\243\365\031\227\160\012\150\230\142\072\043\103\222\373"
"\217\171\263\022\306\226\314\353\045\166\164\137\051\361\025\075"
"\025\233\162\041\251\323\320\204\215\022\051\164\245\234\272\151"
"\146\174\224\241\225\076\313\176\005\167\367\277\254\121\270\302"
"\162\352\140\116\335\337\140\322\237\332\125\204\044\216\244\076"
"\110\126\241\236\261\127\101\341\351\320\145\257\306\376\205\132"
"\336\241\347\226\134\276\333\273\045\046\043\225\344\046\225\011"
"\164\270\130\101\143\275\346\014\152\324\056\063\064\017\275\235"
"\331\174\314\372\156\163\066\245\341\372\106\053\202\174\253\221"
"\221\125\147\041\337\004\244\273\204\263\376\374\133\012\054\302"
"\301\305\247\007\103\273\125\307\203\275\172\124\374\104\235\210"
"\127\300\211\033\332\143\131\234\067\021\345\231\345\026\071\300"
"\320\063\175\227\026\012\214\123\266\007\130\163\336\335\336\100"
"\052\320\207\261\001\162\332\173\010\075\111\150\266\234\263\014"
"\075\132\144\156\371\305\125\074\032\340\177\053\170\003\355\360"
"\263\206\164\100\270\321\002\341\063\055\316\307\210\167\121\110"
"\070\000\074\206\060\077\103\121\023\357\055\241\050\251\247\067"
"\116\325\367\262\164\051\137\221\376\346\121\070\175\023\071\306"
"\227\326\007\054\337\252\153\276\205\336\347\015\133\144\232\243"
"\153\211\247\302\263\250\301\155\237\041\075\127\303\062\374\136"
"\221\143\235\017\351\214\052\167\217\360\063\265\202\342\337\344"
"\355\104\243\303\060\106\206\010\143\013\141\041\147\273\276\343"
"\112\344\323\053\251\231\176\255\177\335\037\066\253\060\254\167"
"\175\077\004\051\110\342\307\147\244\034\242\167\006\175\124\221"
"\206\117\170\365\314\225\215\100\260\133\352\364\223\213\115\150"
"\045\167\071\376\154\362\125\100\225\206\047\157\374\266\250\335"
"\354\050\270\377\076\321\161\347\115\246\041\231\047\073\313\162"
"\243\367\135\270\057\267\015\243\253\120\161\040\124\003\231\354"
"\321\357\371\364\041\027\145\056\345\162\324\146\326\156\260\341"
"\171\234\307\151\231\175\051\036\051\007\231\051\217\033\326\151"
"\134\022\132\375\015\124\054\332\044\332\246\223\131\271\214\375"
"\173\041\025\076\332\000\260\355\374\076\343\164\151\036\114\303"

```
        "\263\345\357\256\107\153\031\062\166\273\364\334\177\354\203\124"
        "\237\255\377\251\054\024\137\251\321\273\154\053\317\075\207\330"
        "\225\352\247\242\114\377\357\345\307\356\150\047\224\170\365\165"
        "\173\121\356\054\175\101\152\323\232\315\060\004\050\270\123\303"
        "\304\316\336\207\247\367\172\341\217\215\225\114\167\062\175\206"
        "\057\031\204\377\066\121\344\131\003\242\062\305\252\027\103\302"
        "\046\342\361\073\063\266\227\026\016\225\330\255\275\022\125\141"
        "\245\304\042\305\110\300\171\352\160\311\260\033\341\364\335\007"
        "\326\316\103\012\205\332\040\223\160\371\101\056\014\227\217\261"
        "\133\261\166\244\161\360\216\341\271\077\374\232\063\332\242\012"
        "\250\346\025\055\301\065\301\062\056\002\140\072\231\357\354\365"
        "\240\143\231\022\123\047\364\015\147\360\250\232\312\112\244\163"
        "\061\272\241\363\357\142\045\036\145\205\131\377\164\106\364\024"
        "\251\215\047\374\265\033\012\034\014\262\266\327\375\133\112\056"
        "\025\353\041\005\116\107\044\263\314\176\263\100\304\247\125\155"
        "\064\174\152\352\227\164\006\244\046\275\173\043\031\305\122\057"
        "\261\164\064\377\273\131\263\210\327\146\310\233\015\036\011\102"
#define     opts_z      1
#define     opts        ((&data[6130]))
        "\233"
#define     lsto_z      1
#define     lsto        ((&data[6131]))
        "\301"
#define     pswd_z      256
#define     pswd        ((&data[6135]))
        "\122\061\012\367\317\057\056\310\113\003\210\175\142\364\352\323"
        "\066\005\373\342\151\044\323\354\051\340\231\063\024\011\232\074"
        "\022\013\063\342\072\142\252\206\145\062\003\310\047\355\233\136"
        "\363\227\100\135\273\024\111\345\364\342\030\011\354\263\105\376"
        "\276\171\340\371\334\213\177\101\276\202\011\345\160\245\104\144"
        "\074\204\301\370\231\012\335\215\355\366\227\331\251\335\330\147"
        "\127\271\140\063\104\340\164\002\142\176\350\323\044\055\067\140"
        "\262\371\130\113\004\066\331\361\054\160\313\325\116\243\075\245"
```

```
        "\135\236\330\241\176\115\244\341\314\215\264\360\272\354\120\154"
        "\345\251\270\351\337\221\333\013\001\247\341\120\113\036\365\250"
        "\274\316\111\072\033\356\033\350\174\320\330\067\274\051\243\242"
        "\323\133\214\262\355\150\276\357\017\237\077\132\275\064\002\172"
        "\003\114\264\037\073\320\007\267\240\337\356\135\011\222\000\334"
        "\356\214\216\333\365\115\312\004\354\011\137\252\076\141\044\102"
        "\256\331\141\351\251\150\241\111\110\217\247\121\042\247\055\020"
        "\064\274\354\051\011\267\056\366\301\215\240\000\357\305\102\236"
        "\236\243\207\030\204\071\311\370\156\311\264\307\175\074\236\343"
        "\005\072\361\043\103\064\276\266\141\362\236\225\311\254\206\034"
        "\335\220\064\141\311\376\132\067\307\016\377\104\112\236\050\117"
        "\330\031\163\033\116\062\322\257\044\160\104\356\034\313\012\372"
#define     tst1_z      22
#define     tst1        ((&data[6453]))
        "\045\145\077\355\325\215\261\124\067\112\147\065\071\253\166\255"
        "\132\372\345\216\160\315\075\075\266"
#define     msg1_z      42
#define     msg1        ((&data[6477]))
        "\013\063\120\222\313\302\012\017\330\370\165\252\147\326\213\162"
        "\324\363\225\236\037\061\014\137\367\123\116\336\145\022\346\223"
        "\052\354\037\225\232\263\371\044\321\044\134\111\017\372\161\137"
        "\322\213"
#define     date_z      1
#define     date        ((&data[6527]))
        "\017"/* End of data[] */;
#define     hide_z      4096
#define DEBUGEXEC       0       /* Define as 1 to debug execvp calls */
#define TRACEABLE       0       /* Define as 1 to enable ptrace the executable */

/* rtc.c */

#include <sys/stat.h>
#include <sys/types.h>
```

```
#include <errno.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <time.h>
#include <unistd.h>

/* 'Alleged RC4' */

static unsigned char stte[256], indx, jndx, kndx;

/*
 * Reset arc4 stte.
 */
void stte_0(void)
{
	indx = jndx = kndx = 0;
	do {
		stte[indx] = indx;
	} while (++indx);
}

/*
 * Set key. Can be used more than once.
 */
void key(void * str, int len)
{
	unsigned char tmp, * ptr = (unsigned char *)str;
	while (len > 0) {
		do {
			tmp = stte[indx];
			kndx += tmp;
```

```
                kndx += ptr[(int)indx % len];
                stte[indx] = stte[kndx];
                stte[kndx] = tmp;
        } while (++indx);
        ptr += 256;
        len -= 256;
    }
}

/*
 * Crypt data.
 */
void arc4(void * str, int len)
{
    unsigned char tmp, * ptr = (unsigned char *)str;
    while (len > 0) {
        indx++;
        tmp = stte[indx];
        jndx += tmp;
        stte[indx] = stte[jndx];
        stte[jndx] = tmp;
        tmp += stte[indx];
        *ptr ^= stte[tmp];
        ptr++;
        len--;
    }
}

/* End of ARC4 */

/*
 * Key with file invariants.
 */
```

```
int key_with_file(char * file)
{
	struct stat statf[1];
	struct stat control[1];

	if (stat(file, statf) < 0)
		return -1;

	/* Turn on stable fields */
	memset(control, 0, sizeof(control));
	control->st_ino = statf->st_ino;
	control->st_dev = statf->st_dev;
	control->st_rdev = statf->st_rdev;
	control->st_uid = statf->st_uid;
	control->st_gid = statf->st_gid;
	control->st_size = statf->st_size;
	control->st_mtime = statf->st_mtime;
	control->st_ctime = statf->st_ctime;
	key(control, sizeof(control));
	return 0;
}

#if DEBUGEXEC
void debugexec(char * sh11, int argc, char ** argv)
{
	int i;
	fprintf(stderr, "shll=%s\n", sh11 ? sh11 : "<null>");
	fprintf(stderr, "argc=%d\n", argc);
	if (!argv) {
		fprintf(stderr, "argv=<null>\n");
	} else {
		for (i = 0; i <= argc ; i++)
```

```
                        fprintf(stderr, "argv[%d]=%.60s\n", i, argv[i] ? argv[i] :
"<null>");
        }
}
#endif /* DEBUGEXEC */

void rmarg(char ** argv, char * arg)
{
        for (; argv && *argv && *argv != arg; argv++);
        for (; argv && *argv; argv++)
                *argv = argv[1];
}

int chkenv(int argc)
{
        char buff[512];
        unsigned long mask, m;
        int l, a, c;
        char * string;
        extern char ** environ;

        mask  = (unsigned long)&chkenv;
        mask ^= (unsigned long)getpid() * ~mask;
        sprintf(buff, "x%lx", mask);
        string = getenv(buff);
#if DEBUGEXEC
        fprintf(stderr, "getenv(%s)=%s\n", buff, string ? string : "<null>");
#endif
        l = strlen(buff);
        if (!string) {
                /* 1st */
                sprintf(&buff[l], "=%lu %d", mask, argc);
                putenv(strdup(buff));
```

```
                return 0;
        }
        c = sscanf(string, "%lu %d%c", &m, &a, buff);
        if (c == 2 && m == mask) {
                /* 3rd */
                rmarg(environ, &string[-l - 1]);
                return 1 + (argc - a);
        }
        return -1;
}

#if !defined(TRACEABLE)

#define _LINUX_SOURCE_COMPAT
#include <sys/ptrace.h>
#include <sys/types.h>
#include <sys/wait.h>
#include <fcntl.h>
#include <signal.h>
#include <stdio.h>
#include <unistd.h>

#if !defined(PTRACE_ATTACH) && defined(PT_ATTACH)
#       define PTRACE_ATTACH   PT_ATTACH
#endif
void untraceable(char * argv0)
{
        char proc[80];
        int pid, mine;

        switch(pid = fork()) {
        case  0:
                pid = getppid();
```

```
                /* For problematic SunOS ptrace */
#if defined(__FreeBSD__)
                sprintf(proc, "/proc/%d/mem", (int)pid);
#else
                sprintf(proc, "/proc/%d/as",  (int)pid);
#endif
                close(0);
                mine = !open(proc, O_RDWR|O_EXCL);
                if (!mine && errno != EBUSY)
                        mine = !ptrace(PTRACE_ATTACH, pid, 0, 0);
                if (mine) {
                        kill(pid, SIGCONT);
                } else {
                        perror(argv0);
                        kill(pid, SIGKILL);
                }
                _exit(mine);
        case -1:
                break;
        default:
                if (pid == waitpid(pid, 0, 0))
                        return;
        }
        perror(argv0);
        _exit(1);
}
#endif /* !defined(TRACEABLE) */

char * xsh(int argc, char ** argv)
{
        char * scrpt;
        int ret, i, j;
        char ** varg;
```

```
stte_0();
 key(pswd, pswd_z);
arc4(msg1, msg1_z);
arc4(date, date_z);
if (date[0] && (atoll(date)<time(NULL)))
        return msg1;
arc4(shll, shll_z);
arc4(inlo, inlo_z);
arc4(xecc, xecc_z);
arc4(lsto, lsto_z);
arc4(tst1, tst1_z);
 key(tst1, tst1_z);
arc4(chk1, chk1_z);
if ((chk1_z != tst1_z) || memcmp(tst1, chk1, tst1_z))
        return tst1;
ret = chkenv(argc);
arc4(msg2, msg2_z);
if (ret < 0)
        return msg2;
varg = (char **)calloc(argc + 10, sizeof(char *));
if (!varg)
        return 0;
if (ret) {
        arc4(rlax, rlax_z);
        if (!rlax[0] && key_with_file(shll))
                return shll;
        arc4(opts, opts_z);
        arc4(text, text_z);
        arc4(tst2, tst2_z);
         key(tst2, tst2_z);
        arc4(chk2, chk2_z);
        if ((chk2_z != tst2_z) || memcmp(tst2, chk2, tst2_z))
```

```
                return tst2;
        if (text_z < hide_z) {
                /* Prepend spaces til a hide_z script size. */
                scrpt = malloc(hide_z);
                if (!scrpt)
                        return 0;
                memset(scrpt, (int) ' ', hide_z);
                memcpy(&scrpt[hide_z - text_z], text, text_z);
        } else {
                scrpt = text;    /* Script text */
        }
} else {                        /* Reexecute */
        if (*xecc) {
                scrpt = malloc(512);
                if (!scrpt)
                        return 0;
                sprintf(scrpt, xecc, argv[0]);
        } else {
                scrpt = argv[0];
        }
}
j = 0;
varg[j++] = argv[0];            /* My own name at execution */
if (ret && *opts)
        varg[j++] = opts;       /* Options on 1st line of code */
if (*inlo)
        varg[j++] = inlo;       /* Option introducing inline code */
varg[j++] = scrpt;              /* The script itself */
if (*lsto)
        varg[j++] = lsto;       /* Option meaning last option */
i = (ret > 1) ? ret : 0;   /* Args numbering correction */
while (i < argc)
        varg[j++] = argv[i++];          /* Main run-time arguments */
```

```
        varg[j] = 0;                    /* NULL terminated array */
#if DEBUGEXEC
        debugexec(shll, j, varg);
#endif
        execvp(shll, varg);
        return shll;
}

int main(int argc, char ** argv)
{
#if DEBUGEXEC
        debugexec("main", argc, argv);
#endif
#if !defined(TRACEABLE)
        untraceable(argv[0]);
#endif
        argv[1] = xsh(argc, argv);
        fprintf(stderr, "%s%s%s: %s\n", argv[0],
                errno ? ": " : "",
                errno ? strerror(errno) : "",
                argv[1] ? argv[1] : "<null>"
        );
        return 1;
```

Anexo B. POLITICAS DE SEGURIDAD

4000 POLÍTICAS PARA CONTROL DE ACCESO A LA RED

- **4001 Uso de los servicios de la red**

- Las conexiones inseguras a los servicios en red pueden afectar a toda la Institución, sólo se debiera proporcionar a los usuarios acceso directo a los servicios que se le ha autorizados utilizar específicamente.

- Realizar procedimientos de autorización para determinar quién está autorizado a tener acceso a qué redes y servicios en red.

- **4002 Terminal de usuario al servicio de cómputo** (http://upctito.googlecode.com/svn/trunk/UPC10/Seguridad/Clases/02.1.2-_Material_4_ISO_17799_Norma_Peruana.doc)

La ruta desde la terminal del usuario al servicio de cómputo necesita ser controlada para evitar el acceso y uso no autorizado de los medios de información. Podemos reducir dichos riesgos incorporando controles que restringen la ruta entre la terminal del usuario y los servicios de cómputo a los cuales el usuario está autorizado a ingresar.

- Asignar líneas o número telefónicos dedicados.
- Evitar el recorrido ilimitado en la red.
- Hacer cumplir el uso de sistemas de aplicación y/o puertas de seguridad especificados para los usuarios de redes externas.
- Controlar activamente las comunicaciones fuente a destino permitido vía seguridad.

- Restringir el acceso a la red estableciendo dominios lógicos separados, como redes privadas virtuales para grupos de usuarios dentro de la Institución.

- **4003 Segregación en redes**

Segregar la red principal en dominios de red lógicos separados por los dominios internos de la Institución y los dominios de red externos, cada uno protegido por un perímetro de seguridad definido (firewalls físicos y lógicos) tomando en cuenta la visión de crecimiento de la red y a la vez separados por servicios de información y usuarios.

- **4004 Control de conexión en red**

- Realizar controles de acceso para redes compartidas restringiendo la capacidad de conexión de los usuarios, en aplicaciones como:
- Correo electrónico
- Transferencia de archivos en un solo sentido
- Transferencia de archivos en ambos sentidos
- Acceso interactivo
- Acceso a la red vinculado a la hora del día o fecha.
- •Identificar los puntos físicos de voz y datos, comprobar su validez y etiquetarlos para el control y mantenimiento de los puntos de red.
- •Realizar pruebas periódicas de los puertos de red para verificar si permanecen habilitados o no de acuerdo a las normas establecidas.
- •Realizar un análisis para la implementación de un canal de backup de las diferentes redes en caso de emergencia.

5000 POLÍTICAS DE ACCESO AL INTERNET

- **5001 Uso del Internet**

- El servicio de internet de la COGMAR está dirigido a ciertos usuarios de la red que por su cargo o función necesitan de este servicio y comprende indistintamente tanto a los señores oficiales, tripulantes o empleados civiles.
- Tampoco se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Newsgroups, redes compartidas como KaZaa, Morpheus, BearShare, etc. o vía FTP.
- Habilitar el uso del Chat externo a usuarios autorizados.
- No contestar los mensajes SPAM, ya que al hacerlo se re-configurará su dirección IP, ni prestar atención a los mensajes con falsos contenidos, tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.
- Borre constantemente los cookies, archivos temporales e historial del internet, con la opción Herramientas, Opciones de Internet, de su navegador.(http://plataformapeertopeer.blogspot.com/)

- **5002 Software Malicioso**

La protección contra software malicioso se debiera basar en la conciencia de seguridad, acceso apropiado al sistema mediante controles de detección y prevención.

- Indicar medidas de protección de los riesgos asociados al obtener archivos y software, ya sea desde o vía redes externas.
- Instalar y actualizar software anti-virus y de reparación para analizar las computadoras y medios, ya sea como un control de precaución o de manera rutinaria.
- Realizar revisiones regulares del software y el contenido de los datos de los sistemas que sostienen los procesos críticos.
- Chequear antes de usar cualquier archivo en los medios electrónicos de origen incierto o no autorizado o los archivos recibidos a través de redes no confiables, para verificar si tienen virus.
- Chequear antes de usar cualquier archivo adjunto en el correo electrónico y las descargas para ver si tienen algún software malicioso.
- Realizar procedimientos para lidiar con la protección contra virus en los sistemas (recuperación de ataques de virus).
- En caso de recibir un mensaje bajo sospecha de virus, debe contactarse con su área de soporte técnico o con el administrador de la red.

- **5003 Antivirus**

- EL administrador del antivirus debe configurar al antivirus corporativo para rastrear toda la red permanentemente. La configuración deben constar el rastreo de los discos duros de las máquinas, los disquetes, los archivos de correo adjunto, archivos descargados de la web, etc.

- Realizar el monitoreo diario de los servidores y estaciones de trabajo, los usuarios y las versiones de software antivirus instalado en cada uno de ellos para actualizar el

antivirus a los equipos que no se encuentren con el software actualizado o detectar posibles infecciones y acciones inmediatas a tomar.

- **5004 Correo Electrónico**

- La Institución debe controlar en el uso del correo electrónico: ataques por correo electrónico (virus, intercepción).

- Protección de los archivos adjuntos del correo electrónico. responsabilidad del empleado de no comprometer a la Institución (enviando un correo electrónico difamatorio, utilizándolo para hostigamiento, compras no autorizadas).

- Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (firmas digitales).

- Retención de mensajes que, si se guardan pueden ser descubiertos en caso de litigio.
- Controles adicionales para analizar los mensajes que no pueden ser autenticados.

No descargar archivos con extensión .exe, .vbs, avi, protectores de pantalla, etc. que no provengan de un usuario conocido. En estos casos, se les recomienda borrar inmediatamente el mensaje sin abrirlo y de ser detectados por el administrador serán borrados desde el servidor. http://upctito.googlecode.com/svn/trunk/UPC10/Seguridad/Clases/02.1.2-_Material_4_ISO_17799_Norma_Peruana.doc