ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRONICA
ESCUELA DE INGENIERIA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"IMPLEMENTACIÓN DE UN PROTOTIPO MEDIANTE LA UTILIZACION DE SOFTWARE LIBRE PARA EVITAR ATAQUES AL PROTOCOLO ARP EN UNA RED DE AREA LOCAL"

TESIS DE GRADO

Previa a la obtención del Título de

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

Presentado por

ORDÓÑEZ GUEVARA ORLANDO FABRICIO

RIOBAMBA – ECUADOR

- 2012 -

Sin duda son muchas las personas especiales a las que me gustaría agradecer, su apoyo, su amistad, animo y compañía en las diferentes etapas de mi vida.

A dos personas luchadoras, un ejemplo de sacrificio y amor hacia sus hijos, Mónica y Francisco, mis padres, a las niñas de mis ojos mis hermanas y mi familia en general.

A todos los grandes amigos que me ha regalado la vida, y en especial Moni y Daniel por siempre poner su hombro cuando me iba a derrumbar.

A mi director Ing. Daniel Haro y colaborador Ing. Edwin Altamirano por ser las personas que me guiaron con sus sugerencias y consejos en la elaboración de esta tesis, a la Lic. Marianita Benítez por siempre brindarme su ayuda desinteresada a lo largo de toda mi carrera.

Al Divino Niño y la Virgencita de Guadalupe quienes me dan la sabiduría y fuerza para afrontar los duros momentos de mi existir.

Orlando

El presente trabajo lo dedico a mi familia, mi madre quien con su dulzura, confianza y esfuerzo ha sido mi inspiración, mi padre un hombre luchador con el que en conjunto y a base de grandes sacrificios han logrado sacar un hogar humilde adelante.

A Evelyn quien me dio la lección más grande de vida y que me ha hecho valorarla cada día más, a Domenika quien con sus locuras e inocencia siempre logra arrancarme una sonrisa del rostro,

A Marce la mujer que ha estado en las buenas y en las malas conmigo, quien ha sido mi refugio y dueña de mi corazón, con quien a lo largo de varios años hemos tropezado y levantado juntos.

Orlando

FIRMAS RESPONSABLES Y NOTA

NOMBRE	FIRMA	FECHA
Ing. Iván Ménes **DECANO FACULTAD DE INFORMATICA Y ELECTRONICA**	_____	_____
Ing. Pedro Infante **DIRECTOR DE ESCUELA ING. EN ELECTRONICA TELECOMUNICACIONES Y REDES**	_____	_____
Ing. Daniel Haro **DIRECTOR DE TESIS**	_____	_____
Ing. Edwin Altamirano **MIEMBRO DEL TRIBUNAL**	_____	_____
Tlgo. Carlos Rodríguez **DIRECTOR CENTRO DE DOCUMENTACION**	_____	_____

NOTA DE LA TESIS: _____

RESPONSABILIDAD DEL AUTOR

Yo, Orlando Fabricio Ordóñez Guevara, soy responsable de las ideas, doctrinas y resultados expuestos en esta Tesis y el patrimonio intelectual de la misma pertenecen a la Escuela Superior Politécnica de Chimborazo.

ORLANDO FABRICIO ORDÓÑEZ GUEVARA

INDICE DE ABREVIATURAS

ARP	Address Resolution Protocol
MAC	Media Access Control
LAN	Local Area Network
IP	Internet Protocol
VLAN	Virtual Local Area Network
CentOS	Community ENTerprise Operating System
IDS	Intrusion Detection System
MAN	Metropolitan Area Network
WAN	Wide Area network
CAM	Content Addressable Memory
S.O.	Sistema Operativo
SLIP	Serial Line Internet Protocol
PPP	Point to Point Protocol
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
SMPT	Simple Mail Transfer Protocol
RHEL	Red Hat Enterprise Linux
PC	Personal Computer
CD	Compact Disc
DVD	Digital Versatile Disc

INDICE

INDICE DE TABLAS

INDICE DE GRÁFICOS

INTRODUCCIÓN

La seguridad informática en el mundo actualmente es un tema de mucho cuidado, su manejo está basado en la tecnología y el uso de la información, la misma que mucha de las veces necesita ser confidencial. La información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo.

La información es poder, y según las posibilidades estratégicas que ofrece el tener a acceso a determinado tipo información.

En el Ecuador la crisis amenaza con crear una "tormenta perfecta" de riesgos de la seguridad de la información, la fuga y pérdida de datos críticos para las empresas aumenta significativamente en los últimos años y los expertos coinciden en que la información se ha vuelto más vulnerable debido a la actual crisis económica que afecta al mundo entero y de la cual no se escapa nuestro país, donde los despidos masivos y los trabajadores con dificultades económicas incitan a un porcentaje de empleados antes leales a plantearse actividades que a la postre son delictivas.

Por tal motivo se ha propuesto un sistema prototipo, el cual sirve para proteger datos y su integridad en una LAN, que generalmente son de mucha confidencialidad para todos los usuarios que se encuentren haciendo uso de esta, en base a la siguiente planificación estructural.

El capítulo I Marco Referencial se expone el planteamiento del problema, los objetivos y lineamientos con los cuales se va de desarrollar la investigación del proyecto.

En el capítulo II Marco Teórico se realiza una introducción a los conceptos generales necesarios a tomar en cuenta para el diseño de la solución y de las características esenciales de los elementos para realizar su implementación.

En el capítulo III Marco Propositivo se realiza todo el proceso del diseño lógico y físico de la red basada en los requerimientos que debe cumplir el sistema para ser una solución efectiva, se describe la implementación del servidor basado en CentOS 6 así como las instalaciones y configuraciones de ficheros y archivos que deben realizarse para que el IDS funcione a la perfección.

En el capítulo IV Monitoreo y Análisis de la red se establece los parámetros que prueban la efectividad del sistema, que luego de realizar un seguimiento procedemos a analizarlos para obtener las conclusiones acerca de su funcionamiento, y con la ayuda de esto es posible comprobar la hipótesis.

CAPITULO I

MARCO REFERENCIAL

1.1 INTRODUCCIÓN

En el presente capítulo se plantea el problema por el cual se ha optado por el proyecto de implementación de un prototipo mediante la utilización de software libre para evitar ataques al protocolo ARP en una red de área local, además se detalla los lineamientos y directrices que ayudarán a desarrollar el proyecto de una forma eficaz y objetiva. Se define las metas principales de este proyecto para cumplir con la planificación establecida.

1.2 JUSTIFICACION DE LA INVESTIGACIÓN

1.2.1 DEFINICIÓN DEL PROBLEMA

Para que exista comunicación entre computadores en las redes de área local es de uso frecuente el protocolo ARP. Este permite que un computador pueda obtener la dirección física o MAC de otro nodo para completar los bytes del paquete que se desea enviar con la dirección MAC del destinatario y finalmente con esta información, poder realizar el envío.

El protocolo ARP hace uso de cachés en las cuales se guardan los mapeos entre direcciones de red IP y las direcciones físicas de las computadoras de la red. Cabe mencionar que antes de enviar una consulta ARP, el sistema operativo trata de resolver la dirección buscándola en las entradas de la caché ARP del sistema.

ARP funciona correctamente en condiciones normales. El problema se da cuando se hace un uso mal intencionado de este protocolo, y se decide usarlo de tal manera que se pueda cambiar la dirección física de uno mismo, o hacerle creer a otro computador que la dirección física propia es otra diferente (envenenamiento a la caché ARP), con el fin de tomar la identidad de otro nodo en la red y llevar a cabo algún tipo de ataque.

1.2.2 JUSTIFICACIÓN

El protocolo ARP trabaja bien en circunstancias regulares, pero no fue diseñado para lidiar con nodos maliciosos; de esta forma, durante el tiempo entre la transmisión de la consulta ARP y la respuesta, los datos son vulnerables a modificaciones, secuestros o redireccionamiento hacia un tercero no autorizado.

Los distintos ataques que pueden ser realizados a este protocolo, comprometen la seguridad de una red. Es así, que el objetivo de este trabajo de investigación es presentar un esquema para asegurar ARP y combatir todos aquellos problemas de seguridad a los que este protocolo es susceptible, a través de una propuesta económica, eficiente y sobretodo fácil de implementar.

Se espera que esta solución quede como ejemplo o punto de partida para otras personas que deseen tener más control sobre el tráfico de sus redes y no sepan cómo afrontar estos problemas.

1.3 OBJETIVOS

1.3.1 GENERAL

- Realizar la implementación de un prototipo mediante la utilización de software libre para dar solución eficaz a los problemas de envenenamiento al protocolo ARP que se presentan en una red LAN.

1.3.2 ESPECÍFICOS

- Implementar y configurar los equipos que intervienen en el desarrollo del prototipo.
- Verificar el nivel operativo de la red mediante pruebas de software especializado.
- Comprobar la seguridad tanto en el envío como en la recepción de los paquetes para demostrar la confiabilidad del prototipo.
- Realizar pruebas y análisis de los resultados obtenidos.

1.4 HIPÓTESIS

Mediante la implementación de un prototipo para evitar ataques al protocolo ARP en una red de área local se pretende encontrar las principales dificultades que actualmente afectan estas, e implementar en una red pequeña para identificar los problemas de envenenamiento ARP y proponer una solución a los mismos, haciendo uso de herramientas no tan sofisticadas, mediante el uso de software libre.

1.5 METODOLOGÍA

1.5.1MÉTODO DEDUCTIVO

El método deductivo es un método científico que considera que la conclusión está implícita en las premisas. Por lo tanto, supone que las conclusiones siguen necesariamente a las premisas: si el razonamiento deductivo es válido y las premisas son verdaderas, la conclusión sólo puede ser verdadera.

1.5.2 MÉTODO DE LA ABSTRACCIÓN

Es un proceso importantísimo para la comprensión del objeto, mediante el se destaca la propiedad o relación de las cosas y fenómenos.

1.5.3 MÉTODO DE ANALISIS

Proceso de conocimiento que se inicia con la identificación de cada una de las partes que caracterizan una realidad. De esa manera se establece la relación causa/efecto entre los elementos que componen el objeto de investigación.

1.5.4 MÉTODO CIENTÍFICO

El método científico es un proceso destinado a explicar fenómenos, establecer relaciones entre los hechos y enunciar leyes que expliquen los fenómenos del mundo y permitan obtener, con estos conocimientos, aplicaciones útiles al hombre.

CAPÍTULO II

MARCO TEORICO

2.1 INTRODUCCION

En este capítulo se realiza una breve descripción de las redes de datos, sus tipos y protocolos, además de las técnicas existentes de detección, mitigación y prevención contra los ataques de envenenamiento a la caché ARP, también se profundiza más acerca del mismo; se describen los métodos de envenenamiento y se detallan las características que hacen del protocolo, un protocolo inseguro.

2.2 REDES DE DATOS

Una red de datos es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones. Un ejemplo es Internet, la cual es una gran red de millones de computadoras ubicadas en distintos puntos del planeta interconectadas básicamente para compartir información y recursos.

Existen 3 tipos de redes de datos, las mismas que a continuación se detallan:

- **Red de Área Local (LAN):** Las redes de área local suelen ser una red limitada la conexión de equipos dentro de un único edificio, oficina o campus, la mayoría son de propiedad privada.

- **Red de Área Metropolitana (MAN):** Las redes de área metropolitanas están diseñadas para la conexión de equipos a lo largo de una ciudad entera. Una red MAN puede ser una única red que interconecte varias redes de área local LAN’s resultando en una red mayor. Por ello, una MAN puede ser propiedad exclusivamente de una misma compañía privada, o puede ser una red de servicio público que conecte redes públicas y privadas.

- **Red de Área Extensa (WAN):** Las Redes de área extensa son aquellas que proporcionen un medio de transmisión a lo largo de grandes extensiones geográficas (regional, nacional e incluso internacional). Una red WAN generalmente utiliza redes de servicio público y redes privadas y que pueden extenderse alrededor del globo.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este

último, estructura cada red en siete capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

2.3 Protocolos de Red

Los protocolos son reglas de comunicación que permiten el flujo de información entre equipos que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma. El protocolo TCP/IP fue creado para las comunicaciones en Internet. Para que cualquier computador se conecte a Internet es necesario que tenga instalado este protocolo de comunicación

Existen muchos protocolos. A pesar de que cada protocolo facilita la comunicación básica, cada uno tiene un propósito diferente y realiza distintas tareas. Cada protocolo tiene sus propias ventajas y sus limitaciones.

El protocolo ARP tiene un papel clave entre los protocolos de capa de Internet relacionados con el protocolo TCP/IP, ya que permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP. Por eso se llama *Protocolo de Resolución de Dirección* (Address Resolution Protocol). Por tal motivo en este proyecto se hará mucho énfasis en este protocolo ya que es la base de la investigación para poder implementar la solución.

2.4 Definición del protocolo ARP

El propósito del diseño del protocolo ARP es poder obtener la dirección física (dirección MAC de 48 bits) de un computador, dada su dirección lógica (dirección IP de 32 bits). El funcionamiento de este protocolo puede ser

explicado en los dos usos que tiene. El primero es cuando se desea hacer la consulta de una dirección MAC entonces se genera una trama de consulta ARP, y el segundo es cuando se recibe una trama ARP ya sea consulta o respuesta. El protocolo se optimiza con la utilización de cachés ARP. En estas cachés se guarda la correspondencia entre direcciones IP y las direcciones físicas de los nodos de la red. Antes de enviar una consulta ARP, se trata de resolver la dirección buscándola en las entradas de la caché.

2.4.1 Formato de la trama ARP

Una trama ARP consta de 2 partes. La primera, que contiene información de la capa de enlace de datos (Ethernet), mientras que la segunda parte es la parte de los datos ARP. En la Figura II.1. Se muestra el formato de una trama normal de consulta ARP y una trama normal de respuesta ARP con la cabecera Ethernet y a continuación se encuentra los dos usos del protocolo ARP de acuerdo al RFC 826.

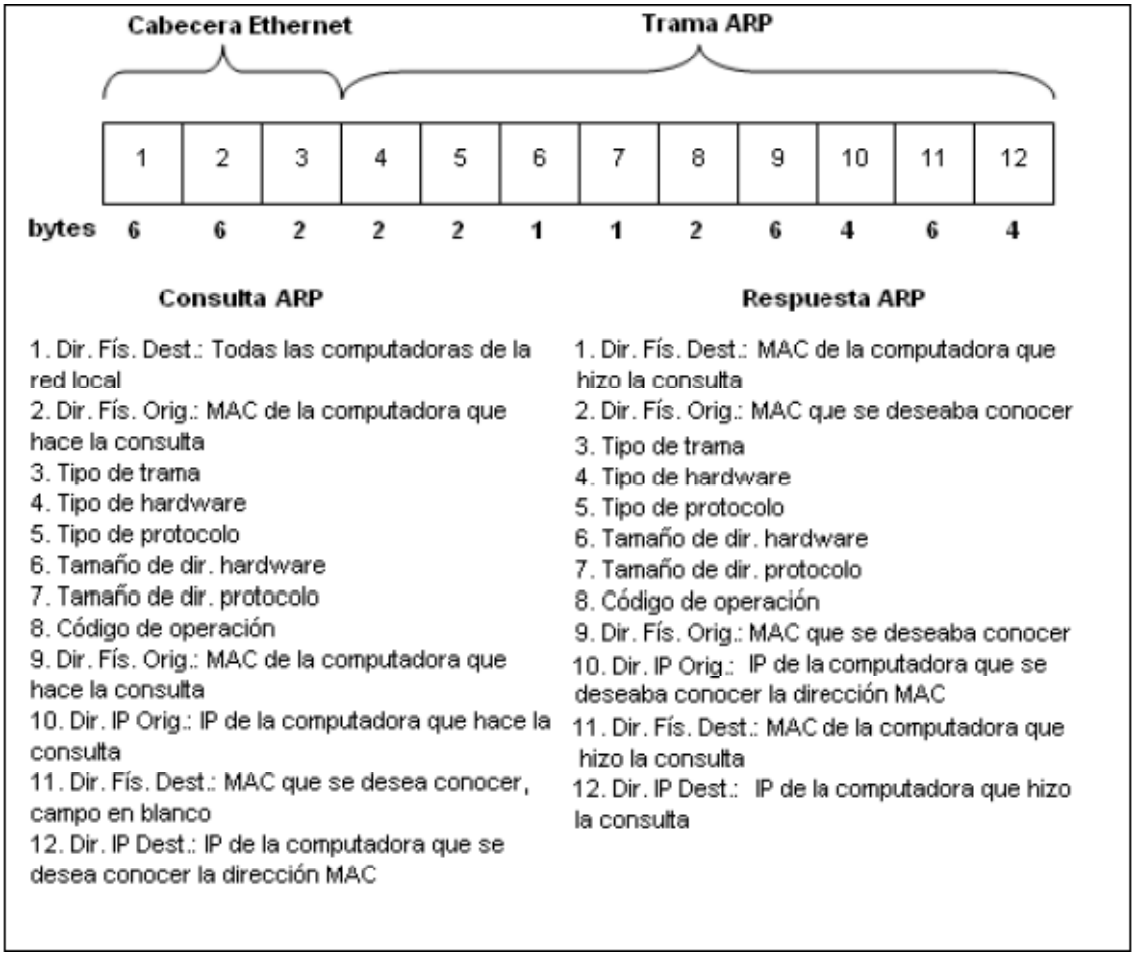


Figura II. 1. Formato de la trama ARP con cabecera Ethernet

2.4.2 Generación de una trama de consulta ARP

Cuando se requiere enviar un paquete a un determinado computador se necesita su dirección física. Por tal motivo en ese instante se realiza la consulta al módulo de conversión de direcciones del sistema (el mismo que nos retornará una dirección física dada una lógica). Si se conoce la dirección lógica del computador al cual se quiere enviar el paquete, el módulo de conversión buscará en su caché la dirección física correspondiente y de poseerla enviará el paquete sin problema a su destino. Caso contrario si no la encuentra, entonces procederá a enviar la trama ARP tipo consulta a manera de broadcast a toda la red de área local, preguntando por la dirección física dada la dirección lógica. En dicha trama, se especifica si es de tipo IP, la longitud en bytes de la

dirección IP, el tipo de operación de la trama que en este caso será de tipo Consulta, entre otros. También se coloca en la trama la dirección física y lógica del computador que hace la consulta, la dirección física que se desea conocer es un campo en blanco sin contenido y el campo final de la trama contiene la dirección IP o dirección lógica de la cual se desea conocer la dirección MAC.

2.4.3 Recepción de una trama ARP

Cuando una trama ARP es recibida, el módulo receptor Ethernet del sistema pasa esta trama al módulo de Resolución de Direcciones, cuyo funcionamiento se detalla a continuación.

Al momento en que se recibe una trama, ARP verifica que la computadora que la recepta trabaje con el mismo protocolo, si es así se setea la bandera Merge_Flag en falso, una vez verificado esto se chequea si en la tabla se conoce ya la dirección lógica y física de quién envía esa trama. Si las conoce se procede a actualizar dichos datos con los nuevos recibidos y se modifica la bandera Merge_Flag a verdadero.

Luego se pregunta si la computadora que recibe la trama tiene la dirección IP del destinatario de la trama, de no ser así se descarta la trama, caso contrario se pregunta por el Merge_Flag. Si este Merge_Flag es falso se procede a actualizar las direcciones de destino tanto física como lógica y el tipo de protocolo en la tabla. Si no, se continúa con el algoritmo sin realizar esta actualización.

Finalmente se pregunta recién si el campo de operación es Consulta, de ser así entonces se hace el intercambio y se llenan los campos del destinatario con las direcciones que se encontraban como fuente y en los campos de dirección tanto lógica como física de la fuente con las direcciones del computador que está recibiendo la trama. Se cambia también el campo de operación con el

número 2, que significa operación de respuesta y se reenvía la trama a su nuevo destino.

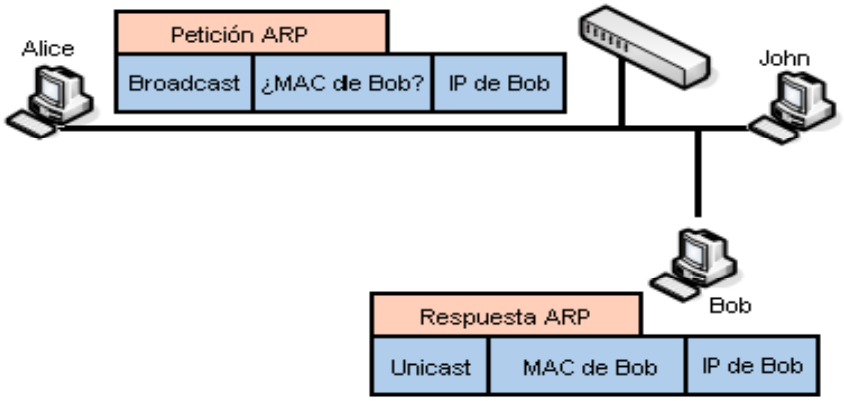


Figura II. 2. Funcionamiento del protocolo ARP

2.5 Riesgos de la Seguridad Informática.

Varios son los riesgos cuando se habla de seguridad informática, entre los cuales se puede nombrar, seguridad física, control de accesos, protección de datos, seguridad en las redes etc. En todos no se puede dejar de tomar en cuenta al protocolo ARP como base fundamental de la seguridad, ya que los ataques que se realizan a este son los que comprometen la seguridad de todo un sistema.

2.6 Métodos de Detección y Prevención a los Ataques de Envenenamiento a la Caché ARP

2.6.1 Envenenamiento a la Caché ARP

El envenenamiento ARP o falsificación ARP, es una técnica usada para infiltrarse en una red Ethernet conmutada, a través de la cual un atacante

maliciosamente modifica el mapeo correcto entre una dirección de protocolo (dirección IP) y la dirección física (dirección MAC) correspondiente en la caché ARP de otro u otros nodos en la red de área local.

El principio del envenenamiento o falsificación ARP es enviar mensajes ARP falsos a la red.

Su finalidad consiste en asociar la dirección MAC del atacante con la dirección IP de otro nodo (el nodo atacado) de la red, de esta manera cualquier tráfico dirigido a la dirección IP de ese nodo, será erróneamente enviado al atacante, en lugar de a su destino real. En la figura II.3. Se muestra como el atacante intenta enmascararse con otra identidad y de esta manera obtener el usuario y contraseña de su víctima.

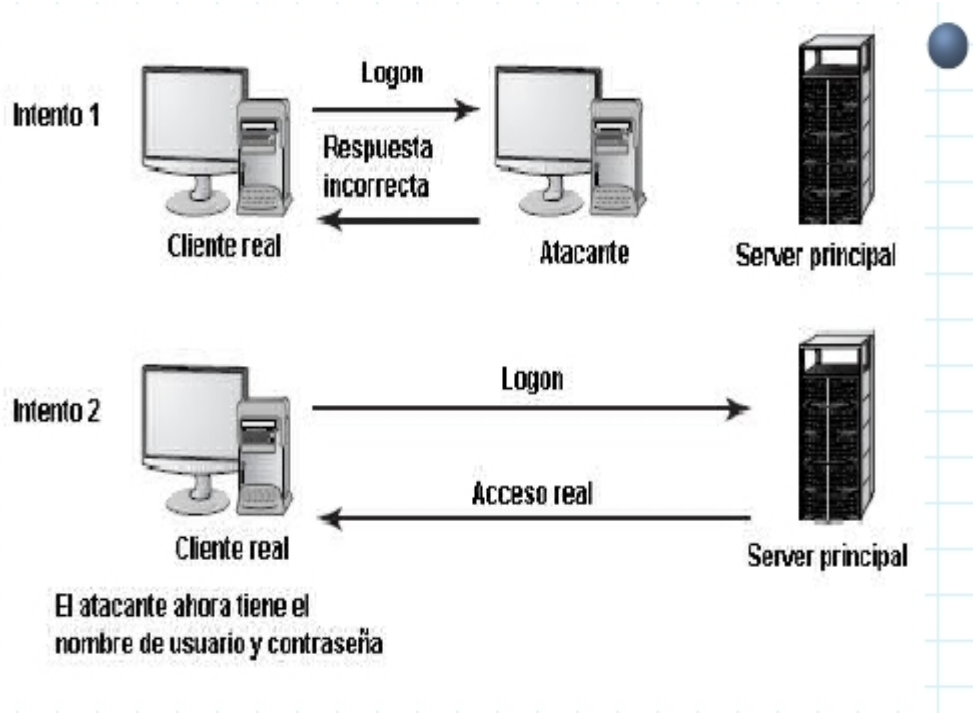


Figura II. 3. Envenenamiento ARP

Cabe mencionar que el envenenamiento más común se da con la distribución de respuestas ARP no solicitadas, que son almacenadas por los nodos en sus

cachés ARP, generando de esta manera el escenario de cachés ARP envenenadas.

2.6.2 Técnicas de Envenenamiento a la Caché ARP

El protocolo *ARP* tiene ciertas carencias que facilitan el uso ilegítimo del mismo para recibir tráfico ajeno. En particular, en el caso que nos ocupa, resultan clave las siguientes características:

- ***Ausencia absoluta de autenticación en el protocolo***.- Una máquina modificará su comportamiento acorde con los paquetes *ARP* recibidos, sin poder determinar de ningún modo la autenticidad de los mismos.
- ***Cachés sujetas a alteraciones externas***.- Es posible modificar los contenidos de una caché *ARP* tan sólo con construir y enviar una petición o respuesta adecuada.
- ***Actualización de las cachés a iniciativa externa***.- Con la técnica de *ARP gratuito*, una máquina puede actualizar las cachés *ARP* del resto en cualquier momento.

Precisamente estas características serán aprovechadas en la técnica del *envenenamiento AR*P o *ARP spoofing* para recibir tráfico ajeno en una red construida con conmutadores. Se basa en ``envenenar'' la caché *ARP* de los dos nodos cuya comunicación se desea intervenir con información falsa, haciéndoles creer que su interlocutor es la máquina atacante. De esta forma, el tráfico generado entre ambas máquinas tiene como destino nuestra propia máquina, y desde ésta las tramas son reenviadas al destino real, evitando así la detección del ataque. Más en detalle, un ataque de envenenamiento *ARP* se produce en las siguientes condiciones:

1. La máquina atacante, conociendo las direcciones IP de los dos nodos cuyas comunicaciones se quieren intervenir, resuelve mediante *ARP*, si es necesario, las direcciones *MAC* que les corresponden.

2. Bien mediante respuestas *ARP* o mediante la técnica de *ARP gratuito*, el atacante modifica el contenido de las cachés de las víctimas de forma que para la dirección IP de su interlocutor se corresponda la dirección *MAC* real del atacante.

3. Cada vez que alguno de los nodos quiera enviar información al otro, resolverá la dirección *MAC* del mismo mediante su caché de *ARP* previamente envenenada, enviando así el tráfico al atacante en vez de al destinatario real.

4. El *switch* enviará las tramas por la boca del destinatario, que en este caso es el atacante. Éste las recibirá y las pasará a la aplicación adecuada, que puede ser un *sniffer* que capture todo el tráfico. Al estar todas las tramas destinadas a su dirección *MAC*, **no** es necesario que la tarjeta de red se encuentre en modo promíscuo.

5. El atacante reenviará el contenido de las tramas al destinatario real. La única diferencia entre la trama original y la modificada es, en un principio, la dirección *ethernet* del destinatario, que varía de la del atacante a la de una de las víctimas.

6. El nodo correspondiente recibirá el tráfico como si nada hubiese ocurrido. El atacante, haciendo uso del *envenenamiento ARP* y la técnica del *hombre en el medio* o *man in the middle* ha interceptado el tráfico sin que ninguno de los interlocutores se percate.

Todos aquellos ataques que pueden ser realizados contra este protocolo, comprometen la seguridad de una red. Es así que existen diversos esquemas para proteger el protocolo ARP ya sea previniendo, detectando o mitigando el problema, actualmente no existe una solución perfecta ya que cada una tiene sus ventajas y desventajas debido a que no han sido probadas con todos los

tipos de ataques ARP, además ser suelen difíciles de administrar y costosas de implementar.

2.6.3 Herramientas Para Detectar Ataques ARP

En la actualidad existen multitud de herramientas gratuitas destinadas a detectar Ataques ARP, lamentablemente se pudo apreciar que la gran mayoría tenían limitaciones o algún problema al detectar todos los diferentes tipos de ataques que una red puede sufrir. A continuación se describe algunas de ellas:

- **ARP Guard**

  Si se habla de “ARP Guard” podemos decir que es un sistema que forma un escudo de protección activa contra ataques internos a la red, incluyendo ataques ARP. Los ataques de suplantación de MAC pueden ser detectados enviando una consulta ARP inversa para una dirección MAC. La respuesta puede ser usada para determinar si una computadora está realizando la clonación (si y solo si el computador siendo clonado no ha sufrido una denegación de servicio o ha sido apagado).

  Lamentablemente esta solución es muy limitada ya que solo detecta este tipo de ataque ARP.

- **Wireshark**

  Otro de los tipos de ataques que puede sufrir nuestra red es el denominado Port Flooding(Inundación de Puerto) , el mismo que consiste en enviar múltiples tramas falsificadas a través de un puerto con el objetivo de llenar la tabla de asignación del switch. Generalmente un switch dispone de una memoria interna denominada CAM (Content-Addressable Memory) donde asigna puertos a direcciones MAC.

Yersinia o Macof permiten generar una inundación (*flooding*) de paquetes con MAC creadas aleatoriamente con el fin de saturar la tabla de asignaciones del *switch*:

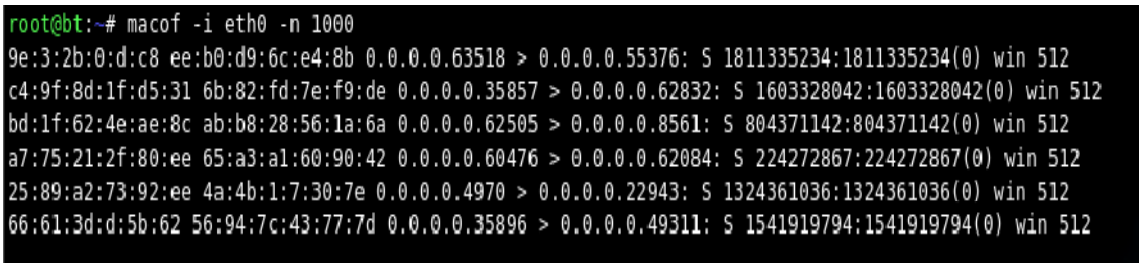


Figura II. 4. Wireshark

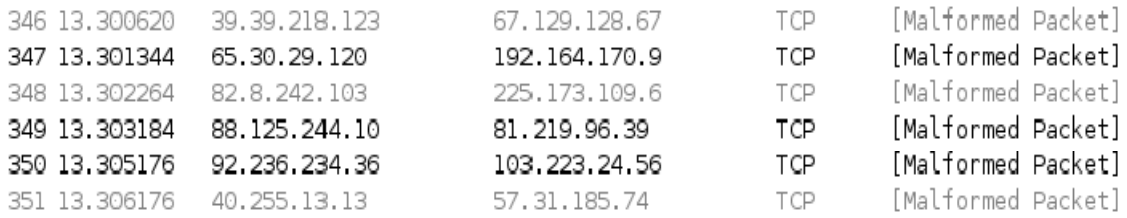
Entonces ahora si se analiza un poco se hará la siguiente pregunta:

¿Qué pasaría si se envían cientos de tramas falsificando la MAC origen del equipo y llenando la tabla CAM?

En ese caso, su comportamiento depende del fabricante. Los switches de baja gama no contienen tablas CAM virtualizadas, es decir, que si la tabla dispone de un número *n* máximo de entradas para almacenar las asociaciones MAC/puerto, y un equipo consigue llenar dicha tabla con *n* entradas, la tabla se llenará y todas las VLANs se verán afectadas.

Para mitigar este tipo de ataques sería sencillo utilizar un analizador de protocolos ya que, únicamente mirando el tráfico generado en ese tramo de red, veríamos gran cantidad de tramas con valores aleatorios.

En el caso de Wireshark veríamos lo siguiente:



346 13.300620	39.39.218.123	67.129.128.67	TCP	[Malformed Packet]
347 13.301344	65.30.29.120	192.164.170.9	TCP	[Malformed Packet]
348 13.302264	82.8.242.103	225.173.109.6	TCP	[Malformed Packet]
349 13.303184	88.125.244.10	81.219.96.39	TCP	[Malformed Packet]
350 13.305176	92.236.234.36	103.223.24.56	TCP	[Malformed Packet]
351 13.306176	40.255.13.13	57.31.185.74	TCP	[Malformed Packet]

Figura II. 5. Captura de paquetes generados por Macof

El motivo por el que se muestra "*malformed packet*" se debe a la forma en la que Macof construye paquetes TCP sin tener en cuenta las especificaciones del protocolo. Como se comentó anteriormente, este ataque daría lugar a una inundación (*flooding*) de paquetes en todos los puertos de todas las VLANs, (en el caso de no contar con tablas virtualizadas) una vez se llenara la tabla de asignaciones. Por lo tanto, en este caso también sería posible dejar escuchando Wireshark en cualquier puerto del *switch* y observar si se están recibiendo tramas no legítimas.

Lamentablemente esta solución también es muy limitada ya que por lo general se la usa únicamente en este tipo de ataque.

.

- **ARP en Redes Conmutadas**

  M. Carnut y J. Gondim propusieron una arquitectura para la detección de ataques ARP en redes conmutadas. Ésta no requiere que software especial sea instalado en los nodos de la red, en su lugar, delega la tarea de detección a una o más estaciones. Sus experimentos demostraron que la solución es muy buena al detectar ataques ARP sin generar falsos positivos, sin embargo los atacantes podrían esconderse tras volúmenes de tráfico sin que pudieran detectarlos por largos períodos de tiempo.

  Estos son los motivos por los que muchas veces el uso de herramientas para detectar ataques ARP resultan no ser efectivas. Para el momento

en el cual el administrador se percate del problema y tome las medidas apropiadas, puede ser muy tarde pues el atacante pudo ya haber obtenido acceso a información sensitiva.

- **Arpwatch**

  La herramienta “Arpwatch”, es usada para detectar tráfico ARP sospechoso. Arpwatch monitorea la actividad Ethernet y mantiene una base de datos de pares <IP, MAC>. Cuando un par cambia, el administrador de la red es alertado vía correo electrónico.

  Veamos la salida que generaría Arpwatch cuando detecta cambios en las asignaciones ARP/IP.

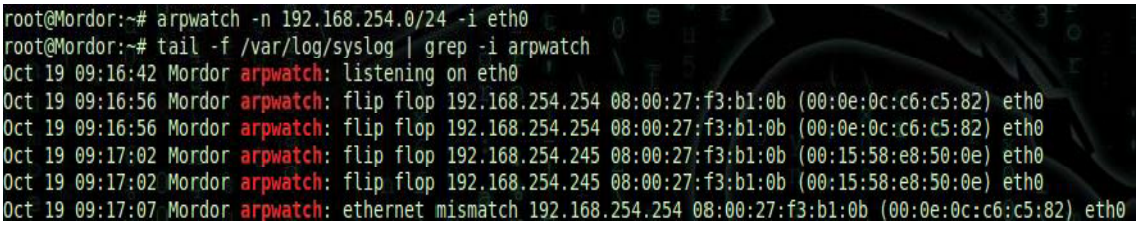


Figura II. 6. Arpwatch

Las 2 primeras líneas muestran un ejemplo de ello: la MAC 08:00:27:f3:b1:0b, perteneciente al atacante, está intentando usurpar la MAC 0:0e:0c:c6:c5:82, que pertenece al *gateway* legítimo, mediante peticiones ARP fraudulentas.

Esta herramienta es ligera y está altamente disponible, pero depende del administrador el poder diferenciar entre eventos no maliciosos y ataques de envenenamiento a la caché ARP, y además de su capacidad para tomar medidas apropiadas cuando un ataque ocurra.

- **IDS's**

  Un Sistema de Detección de Intrusos (IDS) es una herramienta de seguridad que trata de detectar y monitorizar cualquier intento de

comprometer la seguridad en un sistema o una red. En un IDS Se pueden definir previamente una serie de reglas que impliquen una actividad sospechosa en dicho sistema o red y generar una alerta en consecuencia.

Los IDS incrementan la seguridad del sistema o red y, aunque no están diseñados para detener un determinado ataque puede ser configurado para responder activamente al mismo.

Dentro de los IDS's se encuentra el que se va a implementar como el sistema de solución, este se denomina “Snort” el mismo que es un Sistema de Detección de Intrusos que se implementa para detectar ataques al protocolo ARP ya que cuenta con un preprocesador ARP diseñado para generar alertas o alarmas ante ataques de *ARP Spoof*.

2.6.4 Prevención Contra Ataques ARP

Actualmente existen algunos parches para el núcleo de sistema operativo que tratan de defenderse en contra del envenenamiento ARP. Entre estos están:

“Antidote” es un parche, cuando una respuesta ARP nueva anuncia un cambio en un par <IP, MAC>, antidote trata de descubrir si la dirección MAC previa aún no expira. Si la consulta es contestada con la dirección MAC anterior, la actualización es rechazada y la nueva dirección MAC es añadida a la lista de direcciones prohibidas.
Una de las desventajas de este tipo de solución es el soporte para limitados sistemas operativos.

“Anticap” es otro parche para varios sistemas UNIX que previene el envenenamiento rechazando actualizaciones a la caché ARP que contienen

una dirección MAC diferente de la existente en la entrada ARP para la dirección IP.
Lamentablemente al igual que el anterior está disponible para un número limitado de sistemas operativos.

Hace algunos años se propuso una arquitectura para resolver direcciones IP en direcciones MAC en una red Ethernet. Ésta consiste de un servidor seguro conectado en la red y dos protocolos usados para comunicarse con el servidor: un protocolo de invito-acepta y un protocolo consulta-respuesta. El primero es usado por cada nodo en la red para registrar su mapeo <IP, MAC> con el servidor y el protocolo consulta-respuesta es usado por los nodos para obtener la dirección MAC de algún nodo, desde la base de datos del servidor seguro. Este mecanismo no es práctico puesto que requiere modificar la implementación del protocolo ARP de cada nodo en la red local.

Cabe mencionar que también han sido propuestas varias soluciones que involucran técnicas criptográficas para autenticar el origen de las tramas ARP

"*SARP"* es una extensión compatible con ARP que consiste en la criptografía de una clave pública para autenticar las respuestas ARP. Para que esta solución sea implementada en una red local, cada nodo debe ser modificado para que use SARP en lugar de ARP. Adicionalmente debe existir una autoridad de certificación, llamada AKD, la cual es contactada para obtener la llave pública de un nodo y así las respuestas puedan ser autenticadas verificando la firma anexada. Una de las desventajas de esta solución es que AKD constituye un solo punto de fallo en la red.

Expertos hace algunos años también propusieron una nueva arquitectura para asegurar la resolución de direcciones. Su sistema está basado en un árbol hash, un nodo confiable de la red (NC) y un protocolo de autenticación broadcast. Esta solución tiene la ventaja de que no se requiere de operaciones criptográficas simétricas o asimétricas; en su lugar, funciones hash de una sola

vía son usadas. Los nodos pueden continuar trabajando inclusive si el NC ha fallado. El NC solo es necesario cuando una nueva computadora es añadida a la red, o un par <IP, MAC> cambia. En estos casos, el árbol es recalculado y se distribuye al resto de nodos. La mayor desventaja de esta solución es que no es compatible con ARP y puede ser muy ineficiente en redes dinámicas.

Una gran variedad de switches “Cisco” poseen una característica llamada Inspección Dinámica de ARP (DAI). Lo que hace esta función es permitir al switch rechazar tramas ARP con mapeos <IP, MAC> inválidos, para poder detectarlos, el switch usa una tabla construida localmente usando una característica llamada DHCP snooping. Este esquema es una solución bastante buena y efectiva, pero la principal desventaja es el alto costo que tienen los switches con esa funcionalidad.

De las soluciones descritas anteriormente, se puede concluir que ningún esquema ofrece una solución totalmente efectiva o que no posea alguna desventaja para el problema de ataques ARP. El objetivo de este proyecto es presentar un sistema para asegurar ARP y combatir los problemas a los que este protocolo es susceptible, de manera que cumpla con los requerimientos planteados y que la constituyan como una solución ideal y económica.

En el siguiente capítulo se describirán los requerimientos con los que debe cumplir la solución que se está planteando.

2.6.5 Mitigación de Ataques ARP

Una manera de evitar ataques al protocolo ARP es que la red sea dividida en un gran número de subredes con una pequeña cantidad de nodos en cada una, la desventaja, son los altos costos administrativos que puede involucrar esta medida.

Ebtables es una utilidad de Linux usada para crear dispositivos de puenteo programables, permite realizar filtrado a nivel de tramas Ethernet, entre otras cosas. Ebtables puede ser usado para implementar mecanismos de prevención contra ataques ARP. Con esta solución, se podrían filtrar los mensajes ARP que pasan a través del nodo en donde se configuran las reglas de filtrado, mientras que otras áreas de la red permanecerían desprotegidas. Esto representa una desventaja. Adicionalmente, las reglas de Ebtables para prevenir ataques ARP no están ampliamente disponibles, y el administrador de la red tendría la tarea de realizarlas, el cual podría cometer errores al momento de implementar el puente.

Una de las variantes de los ataques ARP usa clonación de dirección MAC para suplantar la identidad de un nodo en la red. La mayoría de los switches implementan una característica llamada seguridad de puerto “port security” basada en direcciones físicas estáticas.

Estos ataques pueden ser prevenidos por el mecanismo de seguridad de puerto. Cuando en el switch está habilitada esta característica, ésta se asegura de que un número limitado de direcciones MAC sea usado en un puerto físico del mismo. De esta forma, si el número límite es uno, un switch puede efectivamente prevenir que un atacante clone la dirección física de otro nodo en la red. Esta solución es muy eficiente, sin embargo no previene otros tipos de ataques ARP y además requiere de administración, aún más si los usuarios son móviles dentro de la red local.

Algunos sistemas operativos como Solaris, aceptan respuestas ARP solo después de que la entrada <IP, MAC> ha expirado. Esta disposición, dificulta al atacante el poder envenenar una caché ARP, pero tampoco es imposible hacerlo. Cuando este tipo de mecanismo es usado, un atacante puede envenenar la caché haciendo que su respuesta ARP llegue antes que la respuesta del nodo legítimo o enviando peticiones echo ICMP forzadas que aparenten salir de una de las víctimas.

La propuesta de M. Tripunitara y P. Dutta consiste en la implementación de una pila de protocolo basado en streams, para bloquear respuestas ARP no solicitadas y enviar alarmas cuando una respuesta no coincide con la entrada existente en la caché ARP. La implementación de este esquema, requiere de su instalación en cada uno de los nodos de la red. La principal desventaja de esta solución es que al depender de duplicados para detectar ataques, no los previene ni detecta cuando el nodo siendo suplantado está apagado o enfrenta un ataque de denegación de servicio.

Los métodos nombrados anteriormente para mitigar ataques ARP también presentan limitaciones.

2.7 IDS

Como se mencionó anteriormente, el servidor es el encargado de responder las consultas ARP que realizan las computadoras de la red local. Adicionalmente mantiene actualizada la caché ARP del sistema.

2.7.1 Tipos de IDS

Los IDS se pueden clasificar según el alcance de su protección:

- **HIDS** (*Host IDS*): Protege contra un Host (Servidor o PC). Posibilita la monitorización de gran cantidad de eventos para un posterior análisis detallado de las actividades sospechosas de manera que se determina con precisión cuan involucrados se encuentran los usuarios en una determinada acción. Todo ello ocurre en modo local, dentro del propio sistema.

- **NIDS** (*Net IDS*): Protege un sistema basado en red. Son sniffers del tráfico de red, ya que capturan los paquetes de red y los analizan,

normalmente en tiempo real, según las reglas con las que ha sido configurado en busca de algún tipo de ataque.

- **DIDS** (*Distributed IDS*) Protege un sistema con una arquitectura basada en cliente-servidor formada por un conjunto de NIDS que actúan recopilando toda la información en una base de datos central. La ventaja de este sistema es que cada NID se puede configurar con las reglas específicas de control que se aplicarán a un determinado segmento de red.

También se pueden clasificar según el tipo de respuesta que generan:

- **Pasivos**: En este tipo de IDS, la herramienta recopila los datos que se generan como consecuencia de las reglas que se han configurado y genera las alertas pertinentes, notificando de posibles ataques al administrador de red, en su caso, pero no actúa en consecuencia para evitar el ataque por sí mismo.

- **Activos**: Los IDS activos sí que responden a las actividades sospechosas que han sido configuradas, tratando de evitar el posible ataque, cerrando la conexión, reprogramando el cortafuegos, etc.

Un IDS está conformado por la siguiente arquitectura:

- La fuente de recogida de datos. Estas fuentes pueden ser un log, dispositivo de red, o como en el caso de los IDS basados en host, el propio sistema.

- Reglas que contienen los datos y patrones para detectar anomalías de seguridad en el sistema.

- Filtros que comparan los datos snifeados de la red o de logs con los patrones almacenados en las reglas.

- Detectores de eventos anormales en el tráfico de red.

- Dispositivo generador de informes y alarmas. En algunos casos con la sofisticación suficiente como para enviar alertas via mail, o SMS.

Esto es a modo general. Ya que cada IDS implementa la arquitectura de manera diferente.

2.7.2 Elementos del IDS

El IDS que se va a implementar posee la siguiente arquitectura:

- Módulo de captura del tráfico
- Decodificador
- Preprocesadores
- Motor de detección
- Archivo de reglas
- Plugins de detección
- Plugins de salida

Figura II. 7. Arquitectura del IDS

2.7.2.1 Modulo de Captura de Datos

El módulo de captura de paquetes del sensor se encarga, tal y como su propio nombre indica, de realizar la captura del tráfico que circula por la red, aprovechando al máximo los recursos de procesamiento y minimizando por tanto la pérdida de paquetes a tasas de inyección elevadas.

Para que los preprocesadores y posteriormente el motor de detección puedan conseguir paquetes se deben realizar algunas tareas previas, por lo que se requiere de una biblioteca de sniffing de paquetes externa: libpcap.Libpcap fue escogida para la captura de paquetes por su independencia de plataforma.

Debido a que Snort usa la biblioteca libpcap para capturar paquetes por la red, puede utilizar su transportabilidad para ser instalado en casi todas partes. La utilización de libpcap hace que se tenga un uso realmente independiente de plataforma.

La responsabilidad de capturar paquetes directamente de la tarjeta de interfaz de red pertenece a libpcap. Esto hace que la facilidad de captura para “paquetes raw” proporcionados por el sistema operativo esté disponible a otras aplicaciones.

Un “paquete raw” es un paquete que se deja en su forma original, sin modificar como había viajado a través de la red del cliente al servidor. Un paquete raw tiene toda su información de cabecera de protocolo de salida intacta e inalterada por el sistema operativo. Las aplicaciones de red típicamente no tratan paquetes raw; estos dependen del S.O. para leer la información del protocolo y expedir los datos de carga útil correctamente.

2.7.2.2 Decodificador

El motor de decodificación está organizado alrededor de las capas de la pila de protocolos presentes en las definiciones soportadas de los protocolos de Enlace de Datos y TCP/IP. Cada subrutina en el decodificador impone orden sobre los datos del paquete, sobreponiendo estructuras de datos sobre el tráfico de la red. Snort posee capacidades de decodificación para protocolos Ethernet, SLIP y PPP. Se encarga de tomar los paquetes que recoge el libpcap y almacenarlos en una estructura de datos en la que se apoyan el resto de capas. En cuanto los paquetes han sido capturados, el IDS debe descifrar los elementos de protocolo específicos para cada paquete. El decodificador de paquetes es en realidad una serie de decodificadores, de forma que cada uno descifra elementos de protocolos específicos. Funciona sobre la pila de protocoles de Red, que comienza con el nivel más bajo: protocolos de la capa de Enlace de Datos, descifrando cada protocolo conforme asciende en la pila de protocolos de red. Un paquete sigue este flujo de datos moviéndose a través del decodificador de paquetes, como se puede ver en la figura:

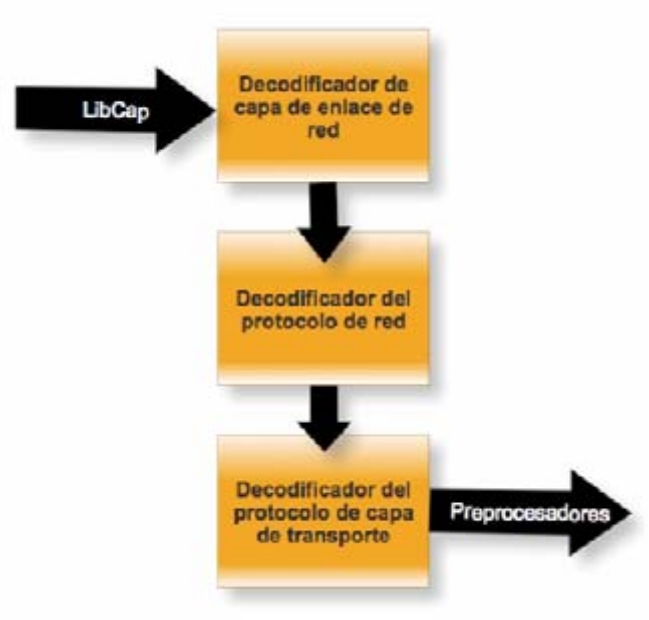


Figura II. 8. Flujo de datos del decodificador

En cuanto los paquetes de datos son almacenados en una estructura de datos están listos para ser analizados por los preprocesadores y por el motor de detección.

2.7.2.3 Procesadores

Para comprender mejor lo que es un preprocesador en primer lugar hay que entender la forma de comunicación de un sistema. Como se puede ver en la figura II. 8, el protocolo TCP/IP es un protocolo basado en capas. Cada capa del protocolo tiene una funcionalidad determinada y para trabajar correctamente necesita una información (cabecera). Por ejemplo, la capa de enlace utiliza para enviar y recibir datos las direcciones MAC de los equipos, la capa de red utiliza las direcciones IP, etc.

Los datos que se transmiten por la red en paquetes de forma individual, pueden llegar a su destino de forma desordenada, siendo el receptor el encargado de ordenar los paquetes y darles sentido.

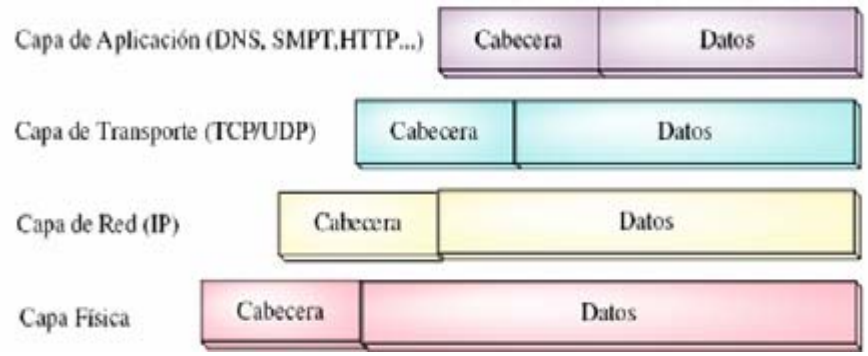


Figura II. 9. Capas TCP/IP

Como el IDS tiene que leer todo el tráfico de la red e interpretarlo también tiene que llevar un control de los paquetes que se envían por la red y así poder darle forma a la información. Por ejemplo, escucha todo el tráfico que tiene como destino una dirección y puertos determinados para ensamblar los datos y así poder interpretarlos. Los Preprocesadores son componentes de Snort que no dependen de las reglas ya que el conocimiento sobre la intrusión depende del módulo Preprocesador. Se llaman siempre que llegue un paquete y se les puede aplicar reglas que estén cargadas en el IDS. Así pues, se encargan de coger la información que viaja por la red de una manera caótica y darle forma para que pueda ser interpretada la información. De esta forma una vez que tenemos los datos ordenados que viajan por la red aplicaremos las reglas (rules) para buscar un determinado ataque. La arquitectura de preprocesadores consiste en pequeños programas C que toman decisiones sobre qué hacer con el paquete. Estos pequeños programas C se compilan junto al IDS en forma de librería. Estos preprocesadores son llamados justo después que el IDS realice la Decodificación, y posteriormente se llama al Motor de Detección. Si el número de preprocesadores es muy alto el rendimiento del IDS puede caer considerablemente. Las configuraciones predeterminadas para estos subsistemas son muy generales, a medida que experimentemos, podremos ajustarlas para obtener un mejor rendimiento y resultados.

2.7.2.4 Reglas (Rules)

Las reglas o firmas son los patrones que se buscan dentro de los paquetes de datos. Las reglas de Snort son utilizadas por el motor de detección para comparar los paquetes recibidos y generar las alertas en caso de existir coincidencia entre el contenido de los paquetes y las firmas. El archivo snort.conf permite añadir o eliminar clases enteras de reglas. En la parte final del archivo se pueden ver todos los conjuntos de reglas de alertas. Se pueden desactivar toda una categoría de reglas comentando la línea de la misma. A continuación, se verán las distintas reglas del IDS, y el formato de las mismas, para poder realizar su configuración.

- **Tipos de Reglas**

Existen cuatro categorías de reglas para evaluar un paquete. Estas cuatro categorías están divididas a su vez en dos grupos, las que tienen contenido y las que no tienen contenido. Hay reglas de protocolo, reglas de contenido genéricas, reglas de paquetes mal formados y reglas IP.

- ✓ **Reglas de Protocolo**.- Las reglas de protocolo son reglas las cuales son dependientes del protocolo que se está analizando, por ejemplo en el protocolo Http está la palabra reservada *uricontent.*

- ✓ **Reglas de Contenido Genéricas**.- Este tipo de reglas permite especificar patrones para buscar en el campo de datos del paquete, los patrones de búsqueda pueden ser binarios o en modo ASCII, esto es muy útil para buscar exploits los cuales suelen terminar encadenas de tipo “/bin/sh”.

- ✓ **Reglas de Paquetes mal Formados**.- Este tipo de reglas especifica características sobre los paquetes, concretamente sobre sus cabeceras las cuales indican que se está produciendo algún tipo de anomalía, este tipo de reglas no miran en el contenido ya que primero se comprueban las cabeceras en busca de incoherencias u otro tipo de anomalía.

- ✓ **Reglas IP**.- Este tipo de reglas se aplican directamente sobre la capa IP, y son comprobadas para cada datagrama IP, si el datagrama luego es Tcp, Udp o Icmp se realizará un análisis del datagrama con su correspondiente capa de protocolo, este tipo de reglas analiza con contenido y sin él.

- **Estructura de las Reglas**

En su forma básica, una regla consta de dos partes:

- Cabecera
- Opciones

En la figura II. 10 se puede ver la estructura que presenta una regla y su cabecera

Figura II. 10. Estructura de una regla

A continuación se va a detallar los distintos componentes que posee una regla:

- o **Cabecera de una Regla**

La cabecera permite establecer el origen y destino de la comunicación, y sobre dicha información realizar una determinada acción. La cabecera contiene algunos criterios para unir la regla con un paquete y dictar qué acción debe tomar una regla. Su estructura es:

<acción> <protocolo> <red origen> <puerto origen> <dirección> <red destino> <puerto destino>

La estructura general de la cabecera de la regla es la que se puede observar en la Tabla:

Estructura de la cabecera de una regla

Acción	**Protocolo**	**Red Origen**	**Puerto Origen**	**Dirección**	**Red Destino**	**Puerto Destino**
alert	tcp	$EXTERNAL_NET	any	—>	$HOME_NET	53

Tabla II. I. Estructura de la cabecera IP

El significado de cada campo es el siguiente:

- **Protocolo.-** Permite establecer el protocolo de comunicaciones que se va a utilizar. Los posibles valores son: TCP, UDP, IP e ICMP.
- **Red de Origen y Red de Destino.**- Permite establecer el origen y el destino de la comunicación.
- **Puerto de Origen y Destino.-** Permite establecer los puertos origen y destino de la comunicación. Indica el número de puerto o el rango de puertos aplicado a la dirección de red que le precede.

  Dirección.- Permite establecer el sentido de la comunicación. Las posibles opciones son: ->, <- y <>

- **Acción.-** Permite indicar la acción que se debe realizar sobre dicho paquete. Los posibles valores son:

    - **Alert.-** Genera una alerta usando el método de alerta seleccionado y posteriormente loggea el paquete.
    - **Log.-** Comprueba el paquete.
    - **Pass.-** Ignora el paquete.
    - **Activate.-** Alerta y luego activa otra regla dinámica.
    - **Dynamic.-** Permanece ocioso hasta que se active una regla, entonces actúa como un inspector de reglas.

o **Opciones de las Reglas**

Las opciones están separadas entre sí, por (;) y las claves de las opciones están separadas por (:). Hay cuatro tipos de opciones:

- **Metadata.-** Proporciona la información sobre la regla pero no tenga alguno afecta durante la detección.
- **Payload.-** Busca patrones (firmas) dentro de la carga útil del paquete.
- **Non-Payload.-** Busca patrones dentro de los demás campos del paquete, que no seancarga útil (por ejemplo, la cabecera).
- **Post-Detection.-** Permite activar reglas específicas que ocurren después de que se ejecute una regla.

A continuación se describen las principales opciones de las reglas:

- **msg.-** Informa al motor de alerta que mensaje debe de mostrar. Los caracteres especiales de las reglas como : y ; deben de colocarse dentro de la opción msg con el carácter \.

- **flow.-** Se usa junto con los flujos TCP, para indicar qué reglas deberían de aplicarse sólo a ciertos tipos de tráfico.
- **content.**- Permite que Snort realice una búsqueda sensitiva para un contenido específico del payload del paquete.
- **referente.**- Define un enlace a sistemas de identificación de ataques externos, como bugtraq, con id 788.
- **classtype.**- Indica qué tipo de ataques intentó el paquete. La opción classtype, usa las classifications definidas en el archivo de configuración de Snort y que se encuentran en archivos como *classification.config.*

La sintaxis de *classification.config es:*

<nombre_clase>, <descripción_clase >, <prioridad_por_defecto >

La prioridad es un valor entero, normalmente 1 para prioridad alta, 2 para media y 3 para baja.
La opción classification para el attempted-admin que aparece en *classification.*config es la siguiente:

config classification: attempted-admin,Attempted Administrator Privilege Gain,1

- La opción **sid** en combinación con la opción *rev*, únicamente identifica una regla Snort, correlacionando el ID de la regla individual con la revisión de la regla.

2.7.2.5 El Motor de Detección

El motor de detección es la parte más importante del IDS. Su responsabilidad está en descubrir cualquier actividad de intrusión existente en un paquete. Para ello, el motor de detección emplea las reglas. Las reglas son leídas en

estructuras de datos internas o cadenas donde son comparadas con cada paquete. Si un paquete empareja con cualquier regla, se realiza la acción apropiada. De lo contrario el paquete es descartado. Las acciones apropiadas pueden registrar el paquete o generar alarmas.

El motor de detección es la parte de tiempo crítico de Snort. Los factores que influyen en el tiempo de respuesta y en la carga del motor de detección son los siguientes:

- Las características de la máquina.
- Las reglas definidas.
- La velocidad interna del bus usado en la maquina del IDS.
- La carga en la red.

El motor de detección puede aplicar las reglas en distintas partes del paquete. Estas partes son las siguientes:

- **La cabecera IP.-** Puede aplicar las reglas a las cabeceras IP del paquete.
- **La cabecera de la capa de Transporte.**- Incluye las cabeceras TCP, UDP.
- **La cabecera del nivel de la capa de Aplicación.**- Incluye cabeceras DNS, FTP, SNMP y SMPT.
- **Payload del paquete.**- Esto significa que se puede crear una regla que el motor de detección use para encontrar una cadena que esté presente dentro del paquete.

Cuando un paquete se captura mediante la librería Libpcap lo primero que se realiza es una decodificación de éste para alinear cabeceras según el protocolo, como se puede ver en el siguiente diagrama de la figura II. 11.

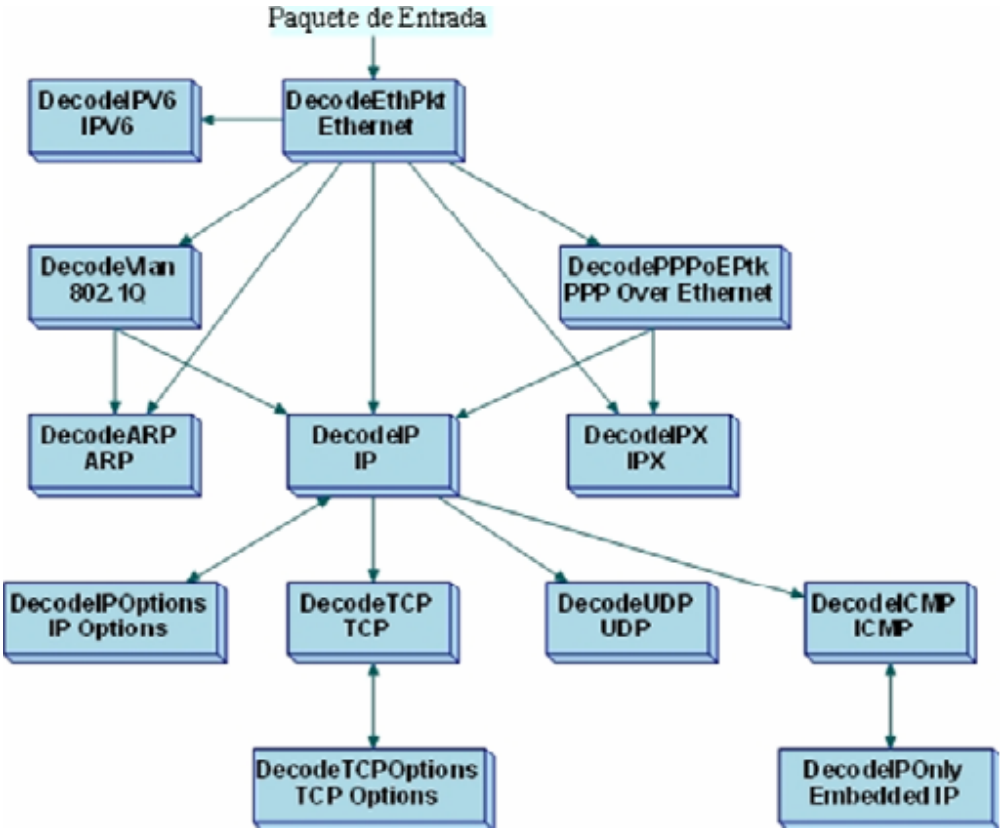


Figura II. 11. Diagrama de decodificación de paquetes mediante Libpcap

En primer lugar se realiza la decodificación de los paquetes, todo depende del protocolo analizado. Posteriormente se realizan las llamadas a los preprocesadores, por cada uno de los que estén instalados en el IDS o preprocesadores propios que hayamos implementado nosotros.

2.7.2.6 Módulos de Salida

Los módulos de salida o plugins pueden hacer diferentes operaciones dependiendo de cómo se desee guardar la salida generada por el sistema de loggin y alerta del IDS. Básicamente estos módulos controlan el tipo de salida generada por estos sistemas.

Existen varios módulos de salida que se pueden utilizar, dependiendo del formato en el que se deseen los datos.

- **Tipos de Módulos de Salida**

  - **Syslog.-** Envía las alarmas al syslog.
  - **Alert_Fast.-** El modo Alerta Rápida nos devolverá información sobre: tiempo, mensaje de la alerta, clasificación, prioridad de la alerta, IP y puerto de origen y destino.
  - **Alerts_Full.-** El modo de Alerta Completa nos devolverá información sobre: tiempo, mensaje de la alerta, clasificación, prioridad de la alerta, IP y puerto de origen/destino e información completa de las cabeceras de los paquetes registrados.
  - **Alert_smb.**- Permite al IDS realizar llamadas al cliente de SMB, y enviar mensajes de alerta a hosts Windows.
  - **Alert_unixsock.**- Manda las alertas a través de un socket, para que las escuche otra aplicación.
  - **Log_Tcpdump.-** Este módulo asocia paquetes a un archivo con formato tcpdump.
  - **Database.-** Snort admite directamente cuatro tipos de salida a base de datos: MySQL, PostgreSQL, Oracle y unixODBC.
    El módulo de salida de base de datos requiere: parámetros y configuraciones, dentro del archivo de configuración y en tiempo de compilación.
  - **CSV.-** El plugin de salida CSV permite escribir datos de alerta en un formato fácilmente importable a una base de datos.
  - **Unified.**- Es un formato binario básico para registrar los datos y usarlos en el futuro. Los dos argumentos admitidos son *filename y limit.*
  - **Log Null.-** A veces es útil ser capaz de crear las reglas que provocarán alertas sobre ciertos tipos de tráfico, pero no causarán entradas en los archivos de log.

- **Eventlog.-** Registra las alertas para visualizarse a través del visor de sucesos de un sistema Windows.

2.8 Servidor de la Red

Para implementar el servidor del prototipo se hace uso de un computador en el que deberá instalarse **CentOS**, el mismo que es una bifurcación a nivel binario de la distribución Linux, Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat.

Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública bajo los términos de la Licencia pública general de GNU y otras licencias. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser bajado y usado por el público.

Lo último mencionado es lo que brinda las facilidades para implementar un sistema que aparte de ser efectivo sea económico y cumpla con todos los requerimientos planteados para evitar la presencia de intrusos en la red.

Actualmente CentOs apareció ya en su versión numero 6 y es la que se va a usar en este prototipo,

No está por demás recalcar que se implementa con el sistema operativo CentOs debido la cualidad que posee de manipular librerías como por ejemplo libpcap para capturar fuente de tráfico.

2.9 Router/Switch Huawei EchoLife HG520c

En cuanto al hardware se ha optado es por el uso del ruteador/switch Huawei EchoLife HG520c el mismo que es una serie de acceso desde el hogar diseñados para la familia y usuarios particulares. Proporciona alta velocidad,

ADSL2 y ADSL2 + interfaces externas de acceso a WAN de banda ancha. Proporciona WLAN, Ethernet y Client, interfaces para la conexión interna con terminales de servicio diferentes de la familia, tales como PC y notebook. Además Funciona con TODOS los sistemas Operativos que manejen TCP/IP: WINDOWS 98,ME, XP64, XP, VISTA, LINUX, MAC, SEVEN7

Figura II. 12.Huawei EchoLife HG520c

2.10 Software Especializado

2.10.1 BackTrack

Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la

auditoría Wireless. Esta dentro de las 30 mejores dentro de la de la famosa lista *"Top 100 Network Security Tools"*

Este será el software que se usará para lograr romper la seguridad de la red, y a la postre demostrar que cuando el prototipo está implementado esto ya no se podrá dar.

CAPÍTULO III

MARCO PROPOSITIVO

3.1. INTRODUCCION

Debido a los contantes ataques a las redes de área local con la técnica de envenenamiento ARP, se propone el diseño de una solución en la cual con herramientas poco sofisticadas y de bajo costo se pretende mantener bajo control y fuera de peligro a la LAN, en este capítulo se van a detallar todos los requerimientos que deberá cumplir el prototipo o sistema que se implementará para que esta sea tomada como una solución ideal, además seguidamente se describirá la topología y el diseño físico y lógico que se plantea.

3.2 Análisis de la situación inicial

El protocolo ARP, es el encargado de convertir las direcciones IP en direcciones de la red física.

El funcionamiento del protocolo ARP es bastante simple. Cuando una máquina desea enviar un mensaje a otra máquina que está conectada a través de una

red ethernet se encuentra con un problema: la dirección IP de la máquina en cuestión es diferente a la dirección física de la misma. La máquina que quiere enviar el mensaje sólo conoce la dirección IP del destino, por lo que tendrá que encontrar un modo de traducir la dirección IP a la dirección física. Esto se hace con el protocolo ARP y aquí radica la importancia del mismo.

Los problemas empiezan a surgir al momento que personas totalmente ajenas a la red intentan suplantar la identidad de otras con el conocido “envenenamiento ARP”, lo que provoca que datos e información que es totalmente confidencial de unos usuarios sea interceptada y llegué a manos de personas en las cuales no deben estar.

El objetivo de esta tesis es lograr mitigar este inconveniente de manera que aunque la red sea atacada, el impostor no logre su cometido y además se logre conseguir saber de dónde se está realizando este ataque y en algún momento descubrir a la persona que desea sacar algún beneficio de datos personales que no le competen.

3.3 Requerimientos del Prototipo

La solución desarrollada necesariamente deberá cumplir con los siguientes requerimientos para que pueda considerarse una solución ideal:

- La solución debe ser fácil de implementar.
- El esquema debe estar ampliamente disponible.
- Se deben minimizar en lo posible requerimientos costosos de hardware.
- No requerir cambios en cada uno de los computadores de la red, por ejemplo, no se debe de realizar la instalación de un software específico en cada nodo, de esta manera se evitará costos administrativos.
- Se debe evitar el uso de técnicas criptográficas, pues éstas disminuirían la rapidez del protocolo.

- Un esquema que evita o detecta ataques ARP es mejor que una técnica que los previene o bloquea.
- Todos los tipos de ataques ARP deberán ser combatidos.

3.4 Objetivo Técnico

El objetivo técnico es proporcionar un medio seguro y confiable para la transmisión de datos, mediante el diseño e implementación de un IDS haciendo uso de software libre y equipos de bajo costo.

3.5 Diseño Lógico

3.5.1Topología

La topología que se usa en el diseño de la red es en “árbol”. Esta topología es también conocida como jerárquica y puede ser vista como una colección de redes en estrella ordenadas en una jerarquía. Éste árbol tiene nodos periféricos individuales que requieren transmitir a y recibir de otro nodo solamente y no necesitan actuar como repetidores o regeneradores.

A continuación se muestra la topología de red que se presenta para la implementación de este prototipo, la misma que consta de una computadora que funcionará como servidor, por lo que posee 2 tarjetas de red un router/switch para repartir el ancho de banda y 3 pc's adicionales de las cuales una de ellas va a ser el atacante y las 2 sobrantes tomarán el papel de victimas.

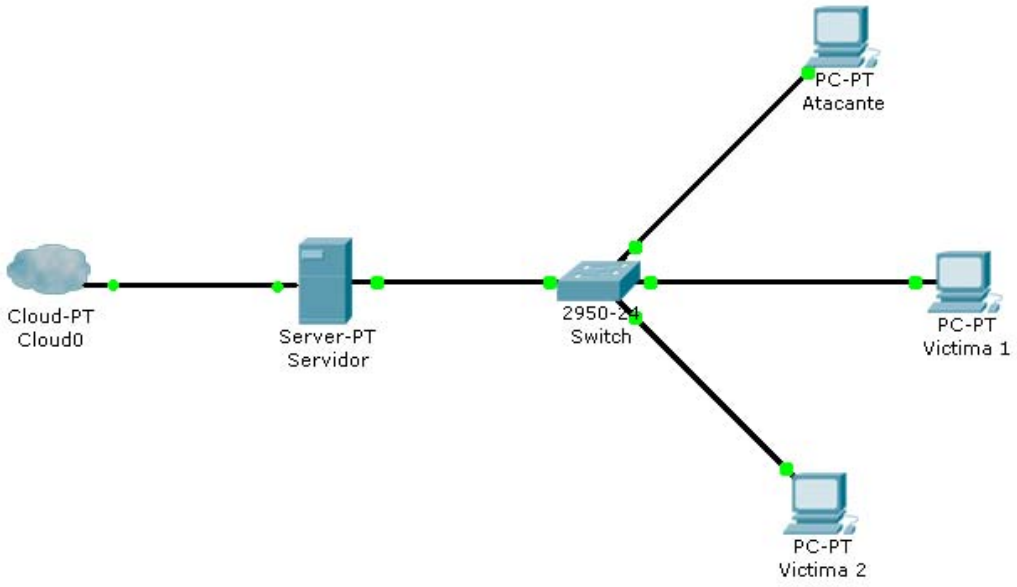


Figura III. 13.Topología de la red

3.5.2 Direccionamiento

DIRECCIONAMIENTO IP DE LA RED		
MÁQUINA	**DIRECCIÓN**	**GATEWAY**
Servidor	192.168.10.1	
Atacante	192.168.10.20	192.168.10.1
Victima 1	192.168.10.2	192.168.10.1
Victima 2	192.168.10.3	192.168.10.1

Tabla III. II.DIRECCIONAMIENTO IP DE LA RED

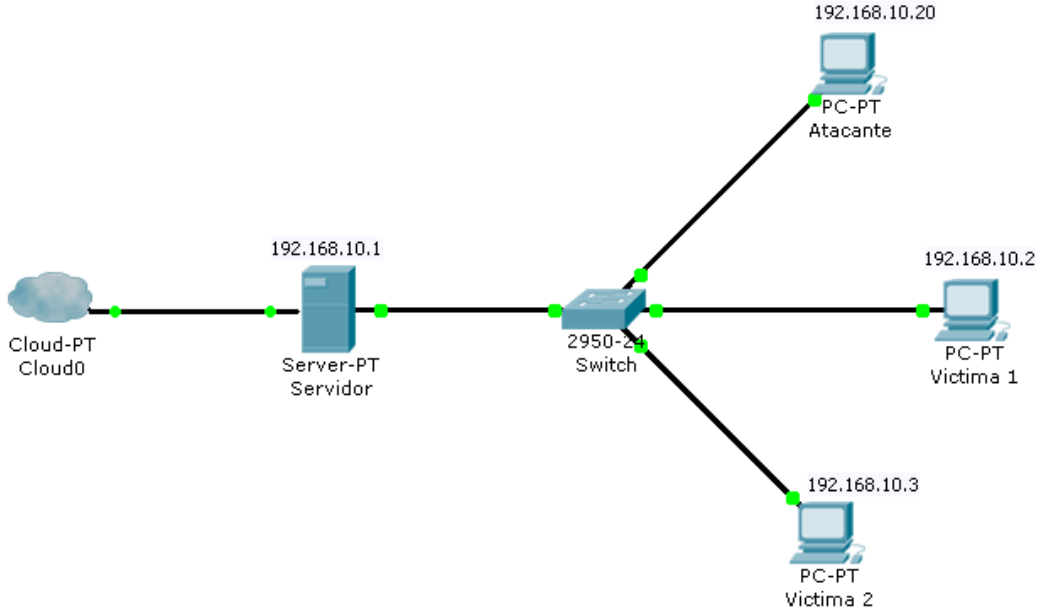


Figura III. 14.Direccionamiento de la red

3.6 Diseño Físico

De manera general la solución la integran los siguientes elementos:

- Computador HP G42-364LA NETWORK, procesador Intel Core i3, 2Gb RAM, 500 GB en disco duro
- Una tarjeta de red genérica adicional conectada al computador que será el servidor de la red.
- Un router/switch Huawei Echolife HG520c
- 3 Computadores adicionales para que tomen el papel de usuarios comunes de la red.

Figura III. 15.Diseño Físico de la Red

En general el sistema evita los ataques ARP contra el Protocolo de Resolución de Direcciones (ARP) en redes de área local.

Un IDS como mencionamos anteriormente implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos o intentos aprovechar alguna vulnerabilidad de un sistema. Todo esto en tiempo real.

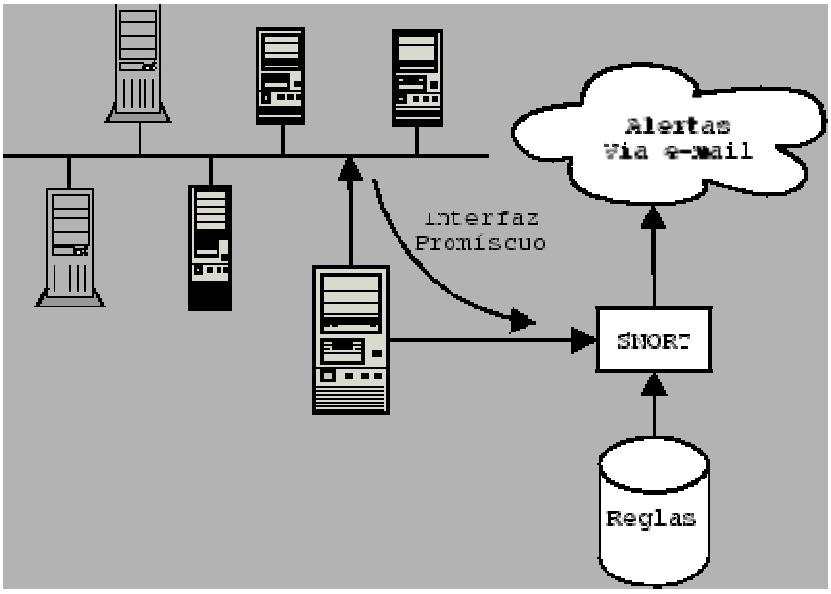


Figura III. 16.Esquema del mecanismo para evitar ataques al protocolo ARP

3.7 Servidor

3.7.1 Instalación de CentOS 6.0

Lo primero que se va a realizar para la implementación del IDS es la instalación de una distribución de software libre denominada Centos en su última versión presentada, Centos 6.0.

No está por demás decir que al ser un software libre, su distribución se encuentra gratuita en su página oficial ***http://www.centos.org/*** y en foros de aquellas personas que gustan usar este software.
Para la instalación del mismo en la computadora que se va a utilizar como servidor se siguen los siguientes pasos:

1. Una vez bajada la versión correspondiente a nuestro servidor comenzamos la instalación arrancando con la ISO grabada en un CD/DVD, nos encontraremos la pantalla de bienvenida en la cual,

seleccionamos la primera opción "Install or upgrade an existing system", y luego esperar que se cargue el modo gráfico de instalación.

Figura III. 17.Pantalla de Bienvenida Para la Instalación del Servidor

2. Ahora se indica si se quiere realizar un Test del CD para verificar que está sin problemas y se puede realizar la instalación, Si se está seguro de tener todo el DVD correcto, se procede a saltar esta opción seleccionando la opción "Skip", en caso contrario si se desea realizar la verificación, escogemos OK.

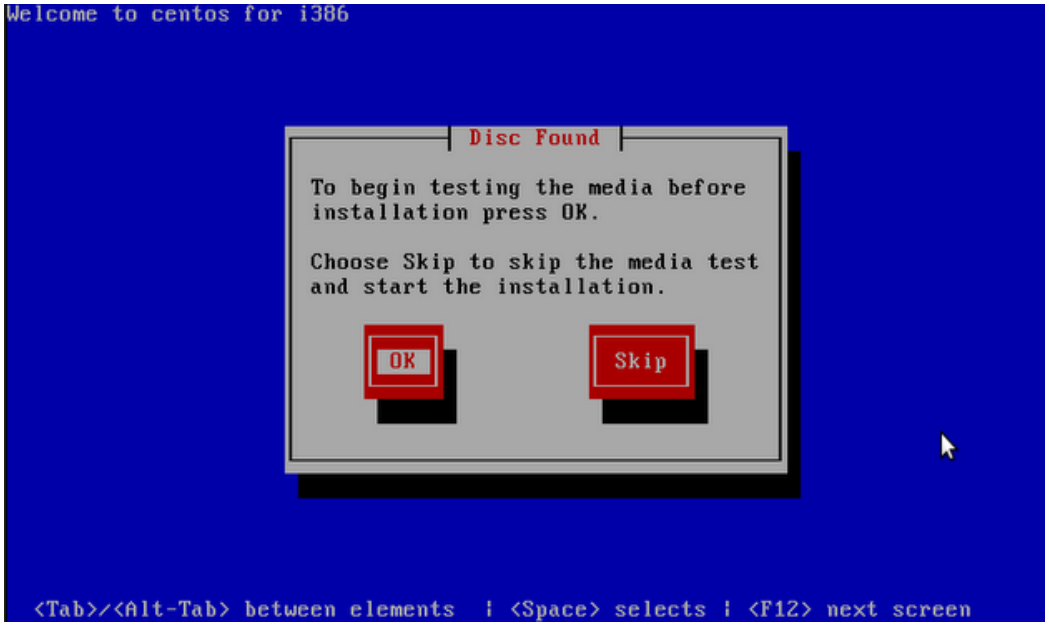


Figura III. 18.Test del CD de Instalación

3. A continuación se selecciona el idioma de la instalación para el sistema operativo en este caso ingles y también el idioma del teclado Latinoamericano.

Figura III. 19.Elección del Idioma Para el S.O.

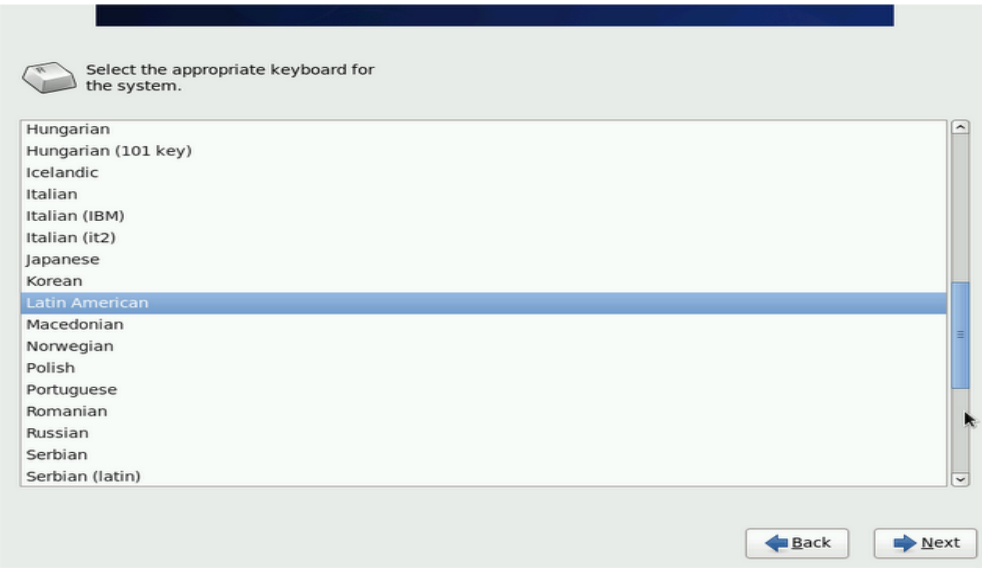


Figura III. 20.Elección del Idioma Para el Teclado

4. Se selecciona el tipo de almacenamiento básico, la primera opción indica que vamos a realizar la instalación en un disco local, si se eligió la 2ª opción sería si se tuviese un almacenamiento externos tipo SAN, en este caso se elige la 1ª opción.

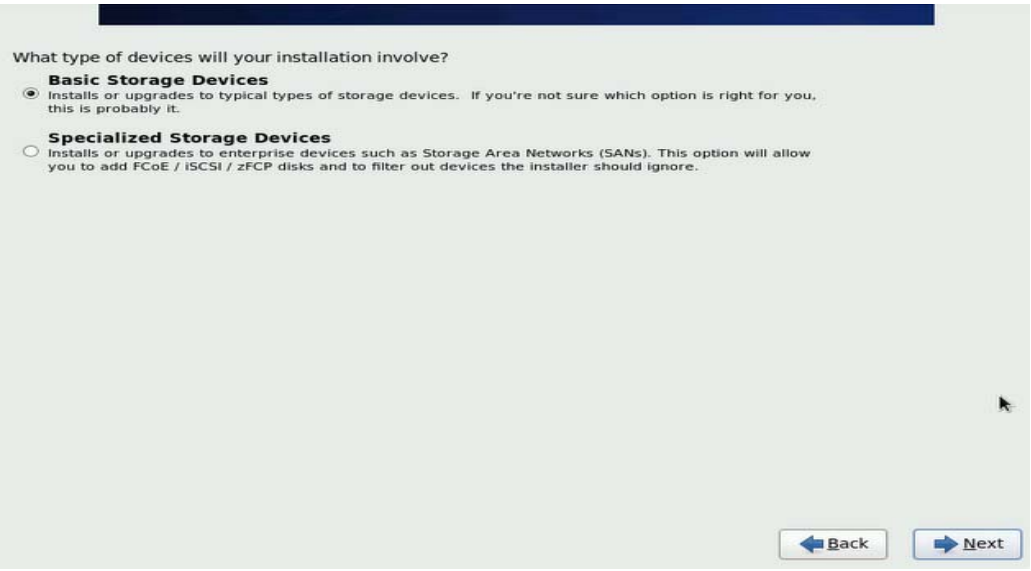


Figura III. 21.Elección del Tipo de Almacenamiento

5. En esta pantalla indica que se quiere reinicializar el disco al ser nuevo, en caso de no existir datos se puede hacer sin riesgo de pérdida de información, pulsar reinicializar todo.

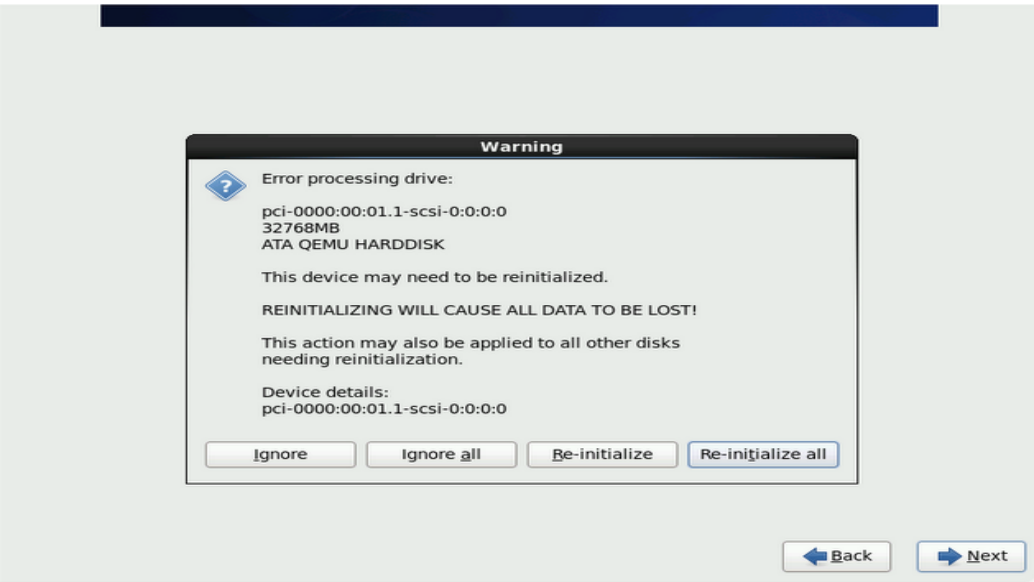


Figura III. 22.Elección para Reinicializar el Disco

6. Lo siguiente será colocar un nombre al servidor (de preferencia cambiarlo luego)

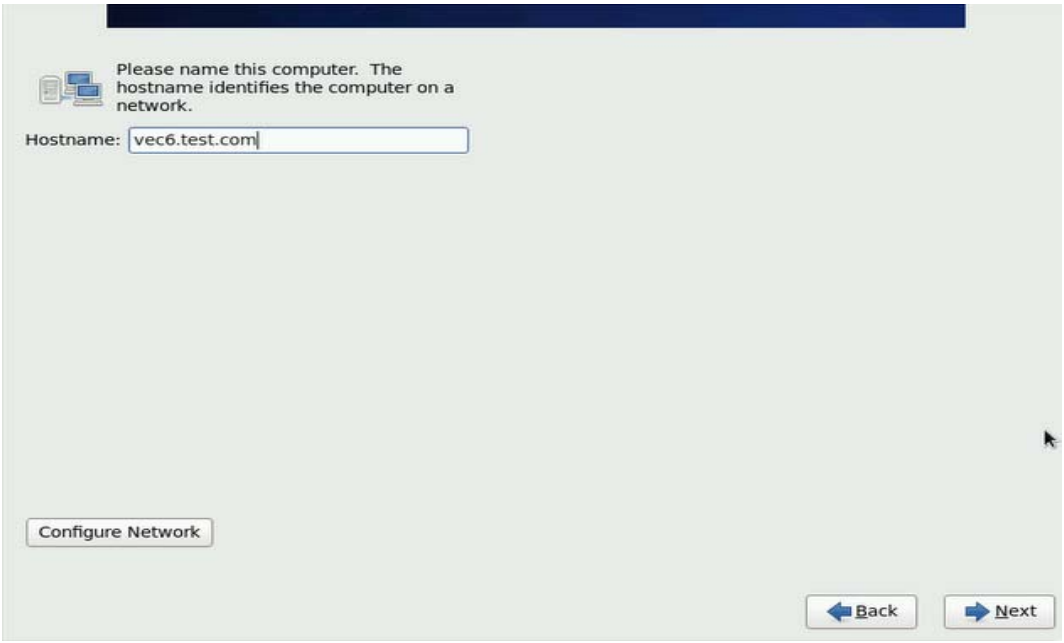


Figura 23.Elección del Nombre del Servidor

7. Seleccionar la localización o zona horaria.

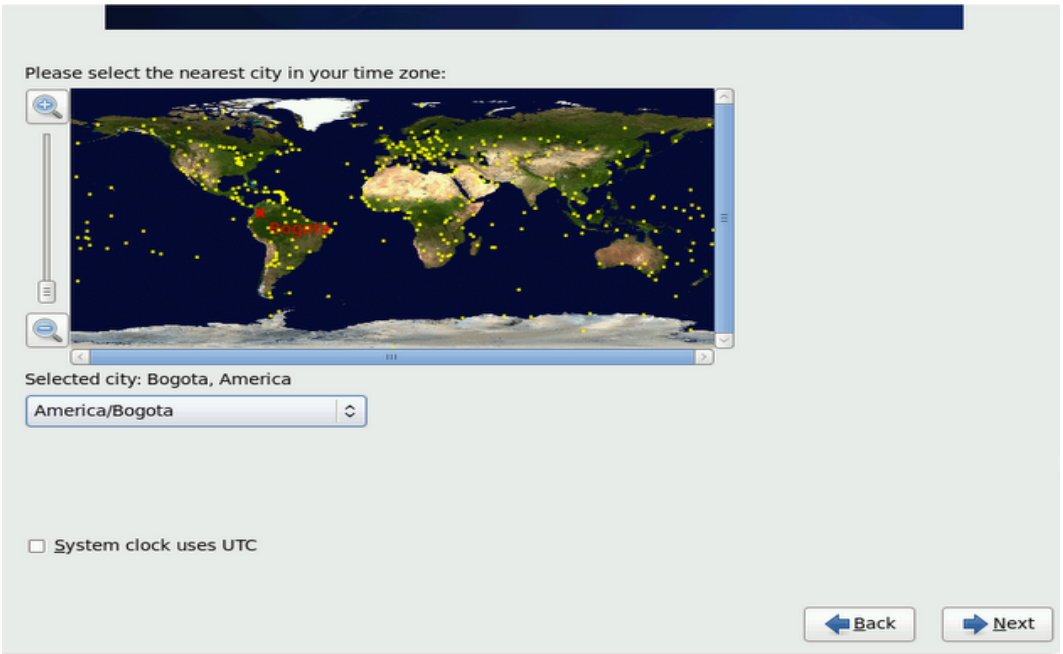


Figura III. 24.Elección de la zona horaria

8. Ingresar la contraseña para root (Administrador)

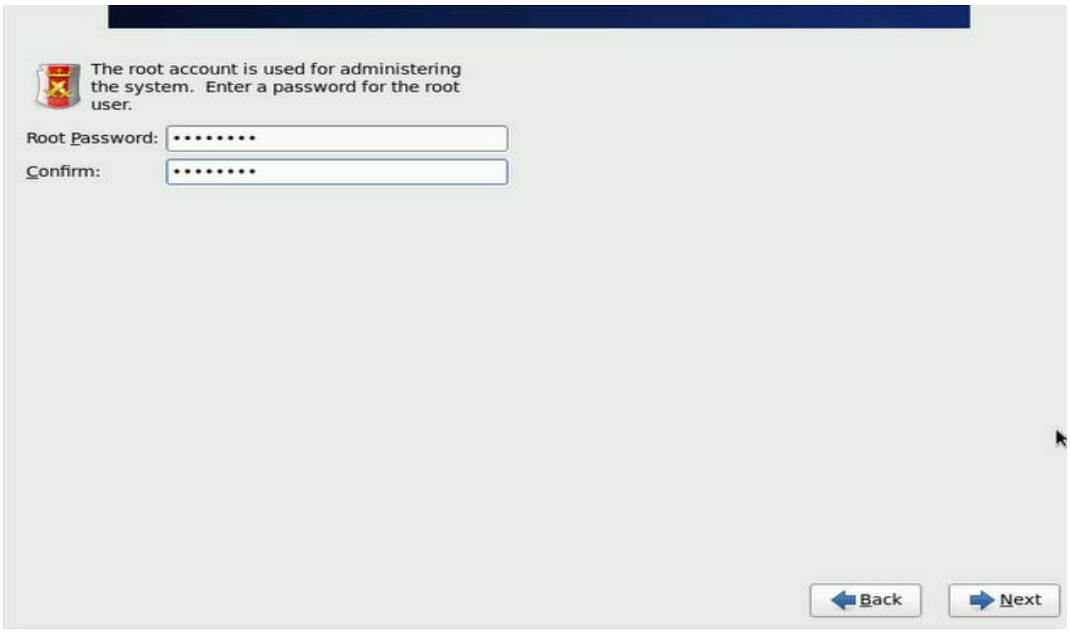


Figura III. 25.Asignación de contraseña para el servidor

9. Elegir el tipo de particionamiento, el mismo que se lo escoge según la disponibilidad en el disco.

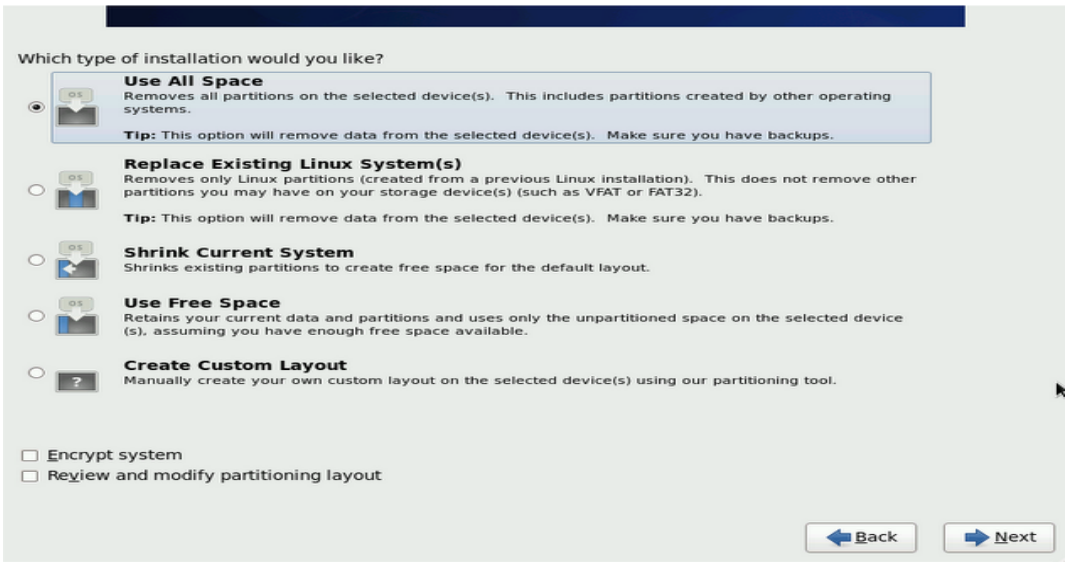


Figura III. 26.Particionamiento del Disco Donde es Instalado el Servidor

10. Escribir los cambios en el disco, al hacer esto formateará la unidad.

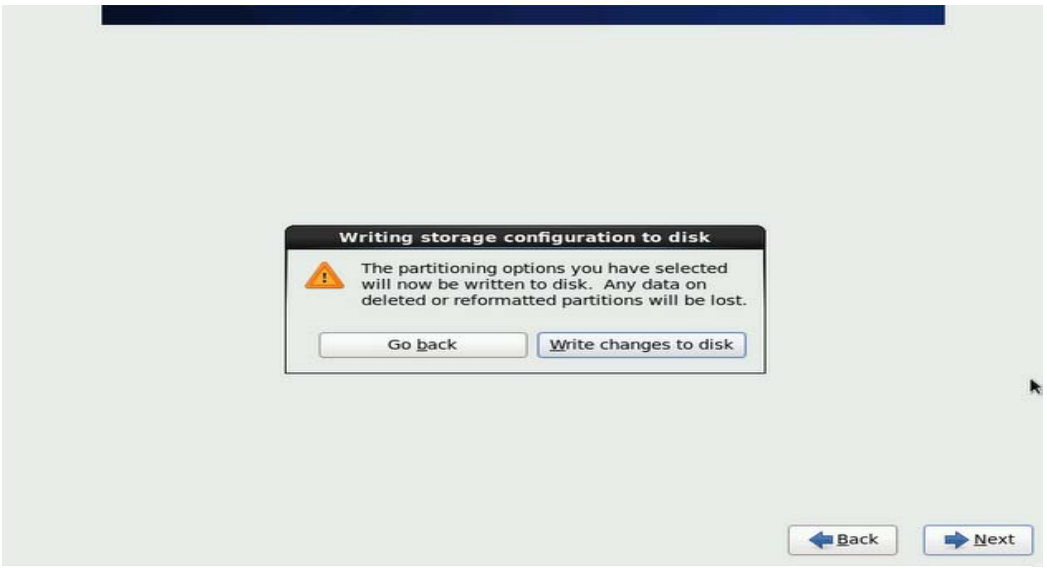


Figura 27.Elección de Cambios en el Disco

11. Este paso es importante, por defecto CentOS realiza una instalación mínima, como se desea que la instalación sirva como un servidor se puede escoger Basic Server (Esto depende ya de la persona que va administrar el servidor).

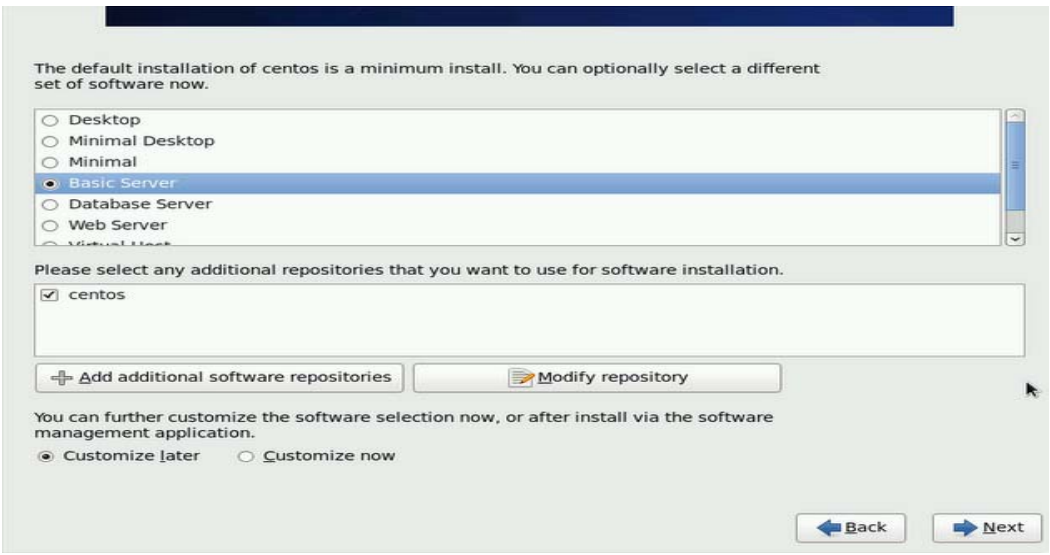


Figura III. 28.Elección del Tipo de Servidor

12. Ahora comienza el proceso de instalación, tardará un poco en función de lo que se haya elegido a instalar.

Figura III. 29.Proceso de Instalación del Servidor

13. Ya terminado el proceso de instalación, reiniciar el equipo y quitar el CD /DVD de la unidad.

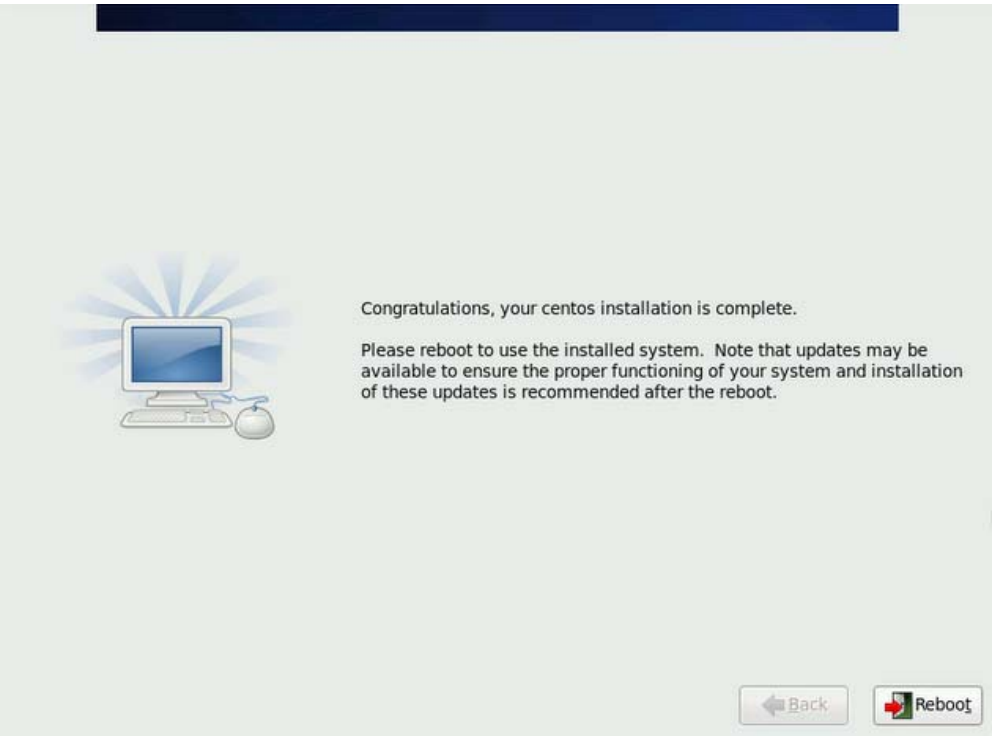


Figura III. 30.Término de la Instalación del Servidor

Una vez reiniciada la maquina ya se tiene el servidor listo para instalar en el, los servicios que son necesarios.

3.7.2 Ubicación, Instalación y Configuración del IDS

3.7.2.1 Ubicación

En primer lugar antes de proceder a la instalación y configuración del IDS, se van a describir las distintas posibilidades para la ubicación de este en la red. La colocación del IDS en la red se debe de realizar en función del tráfico que se quiere vigilar: paquetes entrantes, salientes, dentro del firewall, fuera del firewall, etc.

Se debe de colocar el IDS de forma que se garantice la interoperabilidad y la correlación en la red. Así la interoperabilidad permite que un sistema IDS

pueda compartir u obtener información de otros sistemas como firewalls, routers y switches, lo que permite reconfigurarlas características de la red de acuerdo a los eventos que se generan. Cabe mencionar que se puede colocar el IDS de las siguientes formas:

- Delante del Firewall
- Detrás del Firewall
- Combinación de los dos casos

Esto ya dependerá de los requerimientos que la red necesite.
A continuación se muestra la ubicación que se ha elegido para el diseño de la solución propuesta:

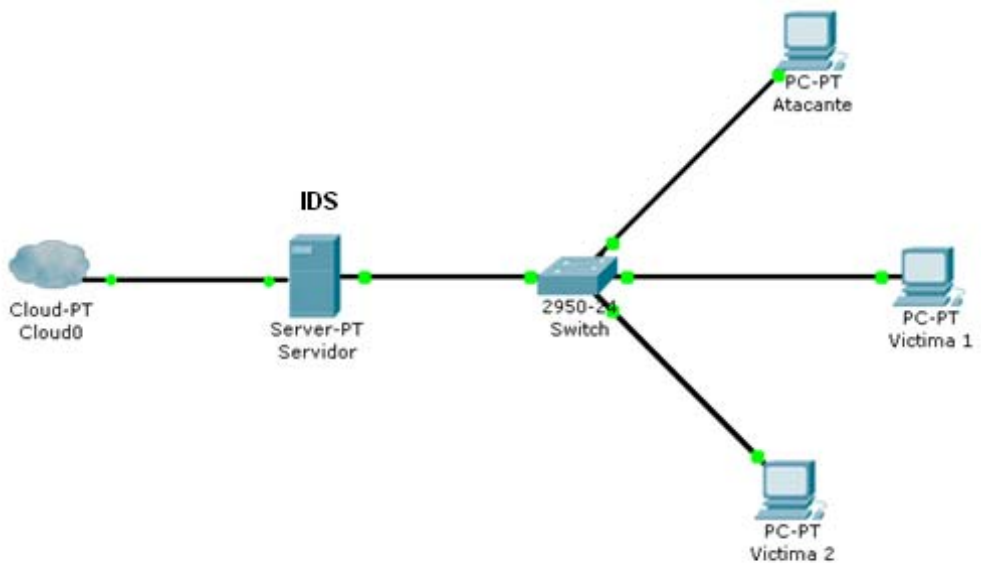


Figura III. 31.Ubicación de un IDS en la red

Una vez que se ha seleccionado la ubicación del IDS de la red (combinación de los dos casos) se procede a su instalación y configuración. A continuación se describe el proceso seguido para ello.

3.7.2.2 Instalación

Al momento se va a describir todos los pasos e instalaciones que se deben realizar en el servidor para configurar el IDS. El sistema de detección de intrusos que se va a configurar se denomina también Snort.

Antes de proceder con esto el primer paso es deshabilitar el firewall y selinux, a continuación se describe qué función tiene cada uno de estos:

El componente SElinux puede deshabilitarse durante el proceso de instalación o bien,si ya se tiene instalado en el sistema, se deberá modificar el fichero ***/etc/selinux/config.***

Cabe mencionar que siempre que digamos que vamos a modificar un fichero se lo realiza con el comando **vi**. En este caso por ejemplo vamos abrir un terminal en nuestro servidor y escribimos lo siguiente:

vi *etc/selinux/config*

Dentro de este fichero modificamos lo siguiente

SELINUX=disabled

SELINUXTYPE=targeted

Con objeto de no tener problemas en el proceso de instalación del sistema, se va a deshabilitar el cortafuegos iptables ejecutando:

iptables –F

A continuación se guarda la configuración con:

iptables-save >/etc/sysconfig/iptables

Se procede a usar el siguiente comando para instalar todos los componentes que se necesitarán, se lo hace con el comando yum de CentOS:

Yum –y install mysql-bench mysql-devel php-mysql gcc pcre-devel php-gd gd glib2-devel gcc-c++ libcap-devel

Este comando sirve para instalar dependencias de la base de datos que necesitaremos más adelante y así también como para instalar el compilador de datos gcc.

A continuación se va a editar el archivo de Securing SSH usando el editor de archivo que nos guste (puede ser el que se mencionó anteriormente “vi”),

/etc/ssh/sshd/sshd_config

Dejándolo de la siguiente manera:

Protocol 2
PermitRootLogin no
PermitEmptyPaswords no

SSH (Secure Shell) es un protocolo que permiten realizar comunicaciones cifradas a través de la red.

3.7.2.2.1 Crear un directorio para usarlo en la instalación

Es una buena idea de colocar todos los archivos descargados en un único directorio para facilitar el acceso. Este directorio ya no serán necesarios después de la instalación está terminada y se pueden extraer de su sistema.
Ahora se va a crear un directorio bajo /root que se va a llamar snortinstall usando los siguientes comandos:

```
cd /root
mkdir snortinstall
cd /root/snortinstall
```

Una vez instaladas las dependencias, para instalar snort hay que seguir los siguientes pasos:

- Se descarga el paquete snort-2.8.6.tar.gz de internet (www.snort.org)
- Se descomprime el paquete ejecutando:

```
tar xvzf snort-2.8.6.tar.gz
```

- Se compila y se instala ejecutando para ello:

```
cd snort-2.8.6
./configure
make
make install
```

En el caso de que se quiera compilar Snort para que tenga soporte para MySQL, se deben de tener en cuenta las siguientes consideraciones:

- Se deben de instalar primero las librerías de MySQL. Para ello se debe de ejecutar:

```
yum install mysql-devel
```

- Finalmente se compila ejecutando el comando:

./configure --with-mysql

make

make install

3.7.2.3 Configuración

En primer lugar para configurar Snort se van a crear los directorios que necesita para trabajar:

- Crear el directorio de trabajo Snort

mkdir/etc/snort

- Ahora crear el directorio donde se van a guardar las firmas

mkdir/etc/snort/rules

- Se crea el directorio donde va a guardar el registro de actividad:

mkdir /var/log/snort

Adduser snort

chown snort /var/log/snort

- Se crea el fichero de configuración local:

touch /etc/sysconfig/snort

- Se copia el ejecutable a su directorio de trabajo:

cp /usr/local/bin/snort /usr/sbin

3.7.2.3.1 Ficheros de Configuración

A continuación se va a copiar los ficheros necesarios para poder trabajar con este IDS.

- Se copia el fichero snort.conf en /etc/snort/ de la siguiente forma:

  cp /root/snort-2.8.0.1/etc/snort.conf /etc/snort/

- Se copia el fichero Unicode.map en /etc/snort:

  cp /root/snort-2.8.0.1/etc/unicode.map /etc/snort/

- Por último copiamos el script de inicio del servidor:

  cp /root/snort-2.8.0.1/rpm/snortd /etc/init.d/

  chmod 755 /etc/init.d/snortd

3.7.2.3.2 Firmas o Rules

En este momento se procede a descargar las firmas de Snort desde www.snort.org. Aquí hay que registrarse primeramente para poder tener acceso a las firmas gratuitas ya que existen unas mejoradas que tienen un costo, para que no se preste para conclusiones aquí está la pantalla y la opción que se debe seleccionar con una pequeña flecha de color negro:

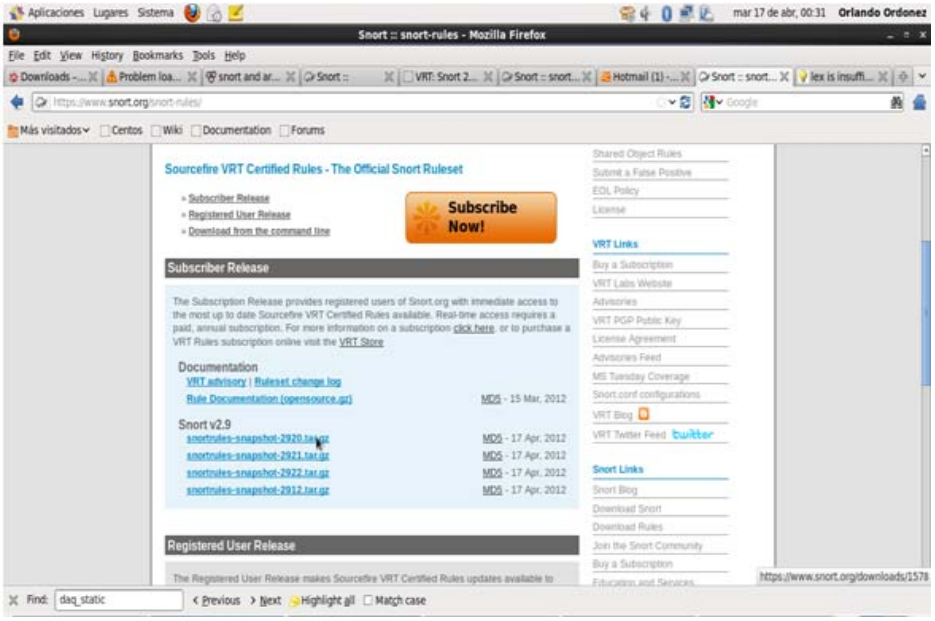


Figura III. 32.Descarda de Snortrules

Cuando se haya procedido ya a descargar las snortrules se continúa con los siguientes pasos:

groupadd snort

useradd –g snort snort –s /sbin/nologin

mkdir /etc/snort/

mkdir /etc/snort/rules

mkdir /etc/snort/so_rules

mkdir /var/log/snort

cd etc

cp /etc/snort*

cd /root/snortinstall

Una vez que haya hecho esto, se puede utilizar el programa scp (copia de seguridad SSH) para copiar estos archivos a través de la instalación de snort nueva con un comando similar al siguiente:

Scp snortrules-snapshot-2860.tar.gz<username>@<ip address of snort sensor>:

Ahora de */root/snortinstall* se va a copiar el archivo usando el siguiente comando

cp /home/<username>/ snortrules-snapshot-2920.tar.gz

En este momento ya se puede descomprimir el archivo y poner los archivos de reglas en el directorio correcto.

tar xvzf snortrules-snapshot-2920.tar.gz

cd ./rules

cp /etc/snort/rules*

cp ../so_rules/precompiled/CentOS-6.0/i386/2.9.2.0/ /etc/snort/so_rules*

Una vez ejecutadas las snortrules empezará la instalación:

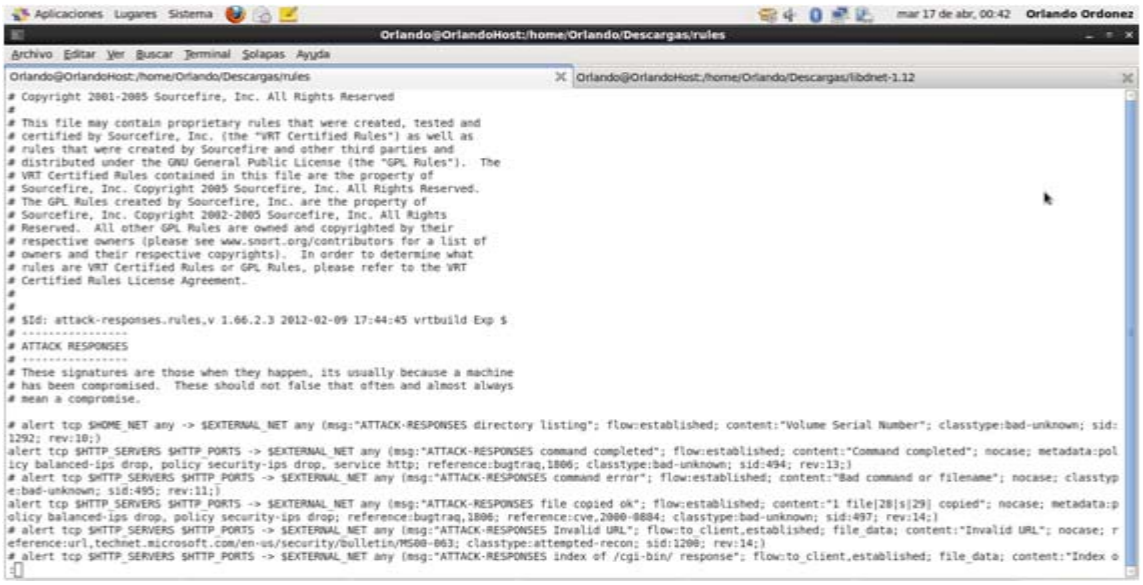


Figura III. 33.Instalación Snortrules

Posteriormente se procede a modificar el archivo snort.conf :

El archivo snort.conf está localizado en /etc/snort. Nuevamente usamos el editor de texto favorito, abrir el archivo y hacer los siguientes cambios.

"var RULE_PATH ../rules" cambiamos esta línea a "var RULE_PATH /etc/snort/rules"

"var SO_RULE_PATH .."so_rules" change this line to "var SO_RULE_PATH

/etc/snort/so_rule"

Un poco más abajo se encuentra la sección de salida (output), ahí agregar la siguiente línea.

Output unified2: filename snort.log,limit 128

3.7.2.3.3 Instalación de la Base de Datos MySQL

MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario, que se utilizará como módulo de salida de las alertas proporcionadas por el IDS. Será necesario tener almacenadas las alertas en una base de datos mysql para el mantener un buen funcionamiento del sistema.

Nota.- La primera vez que se solicite una contraseña simplemente se debe dar enter.
Se necesita crear 2 contraseñas la una será la contraseña de root y la otra va a ser la contraseña de un usuario cualquiera que se le va a llamar en este caso Snort.
Ahora se va a ingresar los comandos para colocar la contraseña de root:

echo "SET PASSWORD FOR root@localhost=PASSWORD('password') ;" | mysql –u root -p

echo "create database snort;" | mysql –u root –p

mysql –u root –p –D snort < ./cshemas/create_mysql

echo "grant create, insert on root. to snort@localhost" | mysql –u root –p*

A continuación hay que ingresar el pasword para el usuario

echo "SET PASSWORD FOR snort@localhost=PASSWORD('password') ;" | mysql –u root -p

echo "grant create, insert, select, delete, update on snort. to snort@localhost" | mysql –u root –p*

Una vez ingresados los comandos anteriores empieza a instalarse la base de datos.

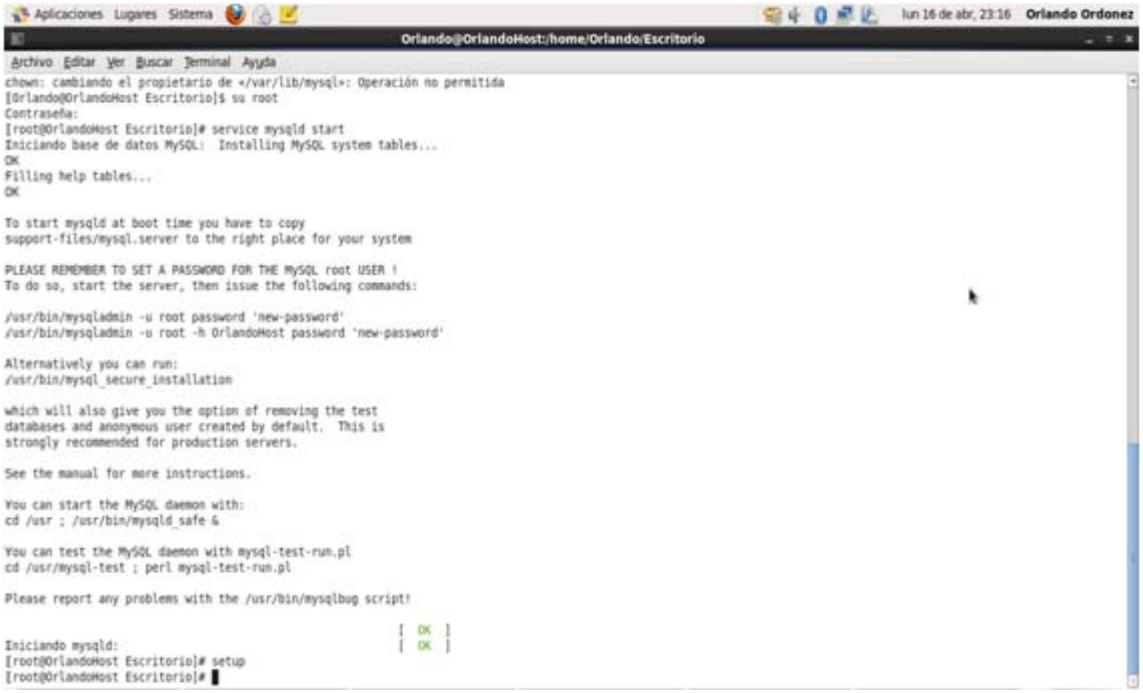


Figura III. 34.Instalación MySQL

3.7.2.3.4 Instalación y Configuración de BASE (Basic Analysis and Security Engine) y ADODB

BASE es una interfaz web en PHP que permite gestionar de una forma fácil y cómoda las bases de datos de seguridad generadas por varios IDS, cortafuegos, y herramientas de motorización.
Para que esta funcione se debe ingresar el siguiente comando:

yum –y install php-pear_numbers_roman php-pear_numbers_words php-pear_image_color php-pear_image_canvas php-pear_image_graph

Para poder utilizar BASE se necesitan tener instalados los paquetes adodb, ahora se procede de la siguiente manera:

- En primer lugar se descarga eel paquete base-1.4.5.tar.gz desde la pagina web http://base.secureideas.net/.
- Se descomprime el paquete en el directorio /var/www/html:

Cp base-1.4.5.tar.gz/var/www/html

Cd /var/www/html

tar xvfz base-1.4.5.tar.gz

Mv base-1.4.5/ base/

- Se procede de la misma manera con el paquete de ADODB

Cp adodb-511.tar.gz/var/www/html

Cd /var/www/html

tar xvfz adodb-511.tar.gz

Mv adodb5/ adodb/

- Ahora si continua configurando BASE

cd /var/www/html

tar xvzf /root/snortinstall/base-1.4.5.tar.gz

Mv base-1.4.5/ base/ (este comando remaplazará el directorio base-1.4.5 a "base")

- Se copia el archivo base_conf.php.dist a base_conf.php usando los siguientes comandos:

cd /base

cp base_conf.php.dist base_conf.php

- Seguidamente se procede a editar el archivo "base_conf.php" e insertamos los siguientes parámetros:

$BASE_urlpath = '/base';

$DBlib_path = '/var/www/adodb';
$DBtype = 'mysql';

$alert_dbname = 'snort';
$alert_host = 'localhost';
$alert_port = “;
$alert_user = 'snort';
$alert_password = ***'password' (colocar la contraseña que se desee)***
/ ARCHIVE DB conection parameters */*
$archive_exists = 0; # Set this to 1 if you have an archive BD

3.7.2.3.5 Proteger el directorio BASE

Para concluir con la configuración del IDS se procede asegurar el directorio BASE. Los siguientes comandos tienen el objetivo de que cuando se vaya ingresar a este directorio solicite una contraseña de acceso. Por lo que se realiza lo siguiente:

- Ingresamos los siguientes comandos en el terminal:

mkdir /var /www/passwords

/usr/bin/htpasswd –c /var/www/passwords/passwords base

Base será el nombre de usuario utilizado para acceder como mencionado anteriormente. Si se quisiera utilizar un nombre de usuario diferente simplemente hay que sustituir ese nombre de usuario en la última línea de comando que acabamos de escribir, Luego se pedirá que introduzca una contraseña que utilizará para esta cuenta.

- A hora se procede a editar el archivo httpd.conf qu ese encuentra en **/etc/httpd/conf**

<Directory "/var/www/html/base">

AuthType Basic

AuthName "SnortIDS"

AuthUserFile /var/www/passwords/passwords

Require user base

<Directory>

Nota.- Se debe tener presente que si anteriormente se cambio el nombre de usuario base, en la línea de comando Require user "base" se tendrá que cambiar esta palabra por el nombre de usuario que se haya escogido.
Finalmente para concluir con la configuración completa del IDS se procede a guardar este archivo y reiniciar el Apache con el siguiente comando.

Service httpd restart

Con esto está terminada la configuración del IDS "SNORT"

3.8 Creación de un Script para la aplicación del IDS.

El script consiste en un programa en texto plano, el cual va a servir para que el administrador del servidor pueda interactuar con el sistema. Este va a ejecutarse en un terminal de CentOS (Ver Anexo 1).

CAPITULO IV

MONITOREO Y ANALISIS DE LA RED

Finalizada la instalación y configuración del IDS se procede a verificar el correcto funcionamiento del prototipo, para lo cual se realiza las respectivas pruebas que valide el funcionamiento del mismo.

4.1 Ejecución de las pruebas

Las pruebas se realizan usando “BackTrack” que es una distribución GNU/Linux pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Esta distribución actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática, y con el se va a comprobar que la seguridad de la red una vez instalado el sistema es mucho más consistente.

Una vez que la maquina es atacada se procederá a la implementación de la solución monitoreándola antes y después del ataque con la finalidad de verificar el impacto puede sufrir una red al no estar segura.

4.2. Ataque a la red Hombre en el Medio

Anteriormente se indico que la dirección MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. El problema empieza cuando una computadora se hace pasar por otra simulando el cambio su dirección MAC.

Para realizar los ataques se va a usar “Backtrack” y se va a infiltrar en la red haciendo un ataque de denominado “MAN ON THE MIDDLE”, con el siguiente comando:

Ettercap –T –q –i eth0 –M arp /192.168.10.1/ /192.168.10.2/

192.168.10.1 -> servidor

192.168.10.2-> máquina a atacar

4.3 Monitoreo de la red

La principal función del IDS es “detectar” todo lo que sucede en la red, todos los movimientos que en esta se da, de donde vienen y hacia a dónde van los paquetes y que objetivo poseen.

La siguiente pantalla muestra lo anteriormente anotado.

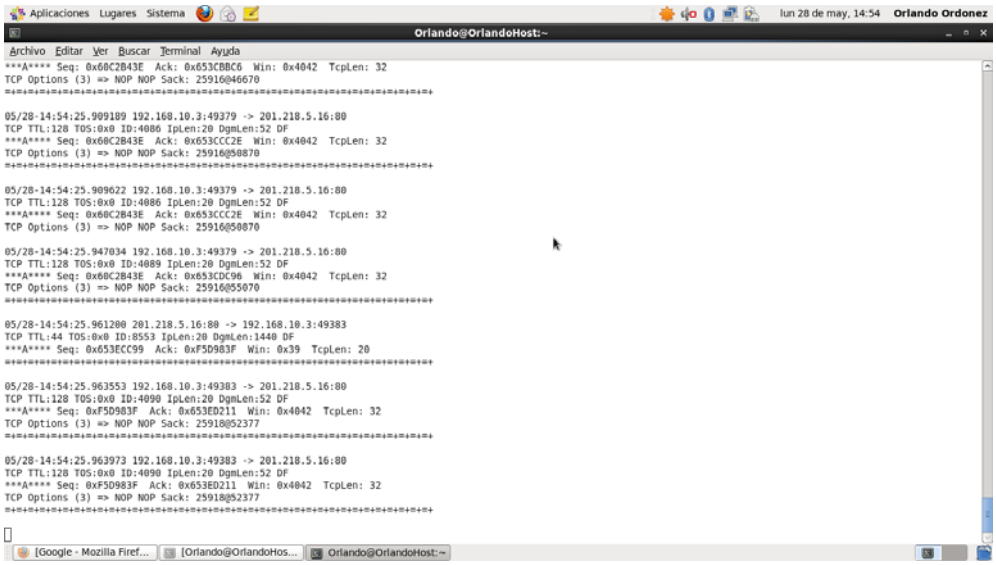


Figura IV. 35.Escaneo de Snort

4.3 Parámetros de evaluación

Después del monitoreo de la red se puede observar los parámetros que el comando snort ha evaluado, siendo algunos de ellos los más importantes, motivo por el cual se los toma en cuenta para valorar la importancia del IDS en la red:

- Ping
- Confidencialidad de los datos
- Integridad de la información
- Disponibilidad de la red

4.3.1. Ping

Dentro del comando ping se valora algunos parámetros, en esta ocasión el parámetro que se utilizará es la latencia, ya que nos indica el tiempo de respuesta de la red, el resultado que se presenta a continuación es fruto de un ping directo desde el servidor hacia una computadora víctima.

- **Sin el prototipo implementado**

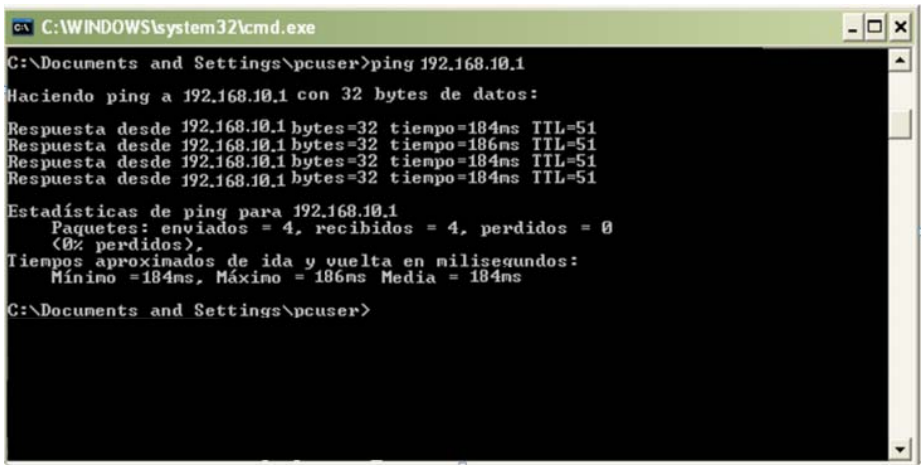


Figura IV. 36.Tiempo de respuesta = 184 ms

- **Con el prototipo implementado**

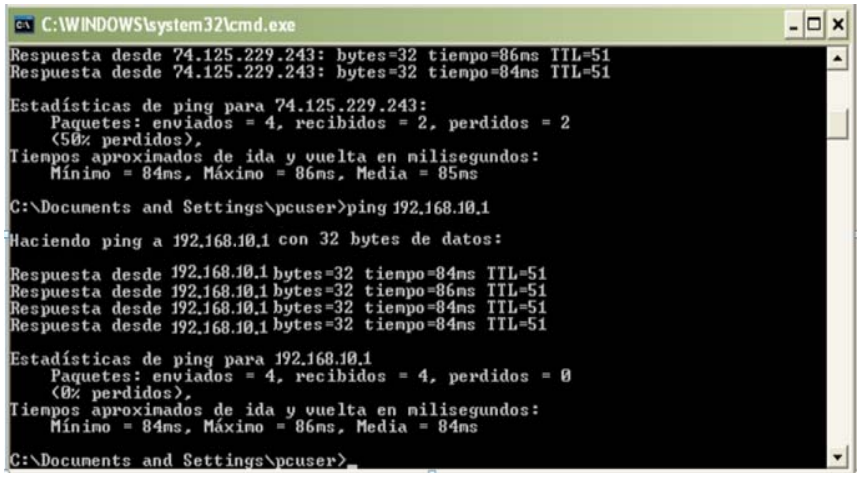


Figura IV. 37.Tiempo de respuesta = 84 ms

4.3.2 Confidencialidad de datos

Es la preservación del acceso a información y recursos únicamente por usuarios autorizados y de la manera autorizada

Se logra a través de:

- Identificación
- Autenticación
- Autorización

.

- **Sin la solución Implementada**

La victima está siendo atacada y su identidad está siendo robada.

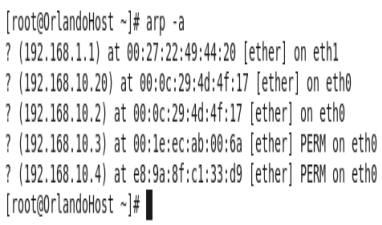


Figura IV. 38.Pantalla duplicación de MAC

En la tabla de ARP que se muestra anteriormente existen 2 computadoras con la misma dirección MAC lo que es imposible que exista ya que esta es única para cada equipo, es así como el intruso ya tomo otra identidad y puede romper la confidencialidad de los datos de la siguiente manera

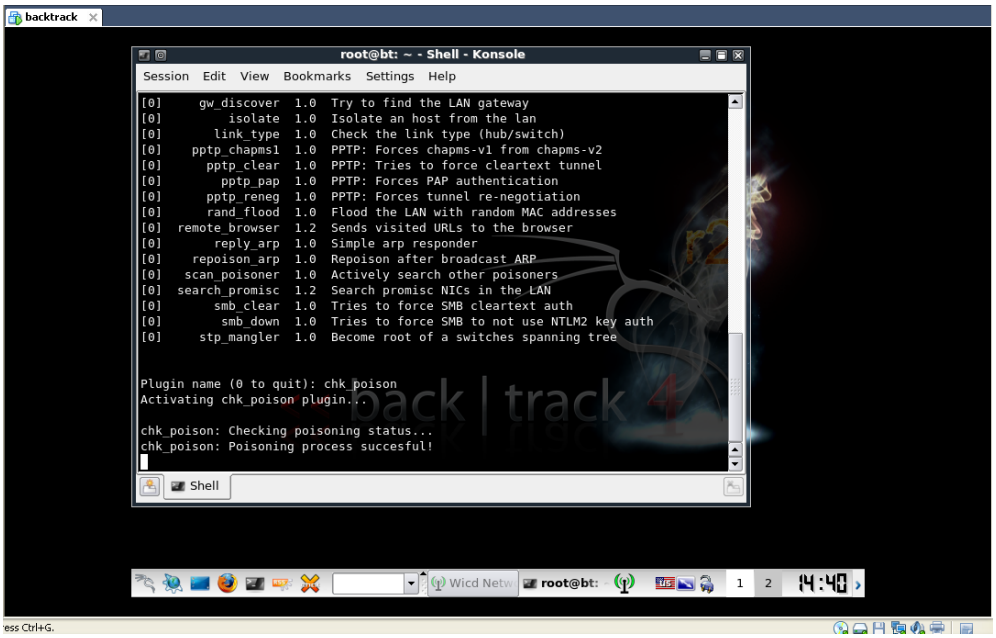


Figura IV. 39.Proceso de Envenenamiento Exitoso Usando "Backtrack"

Por lo tanto si intenta logearse a una página web cualquiera, su usuario y contraseña pueden ser robados.

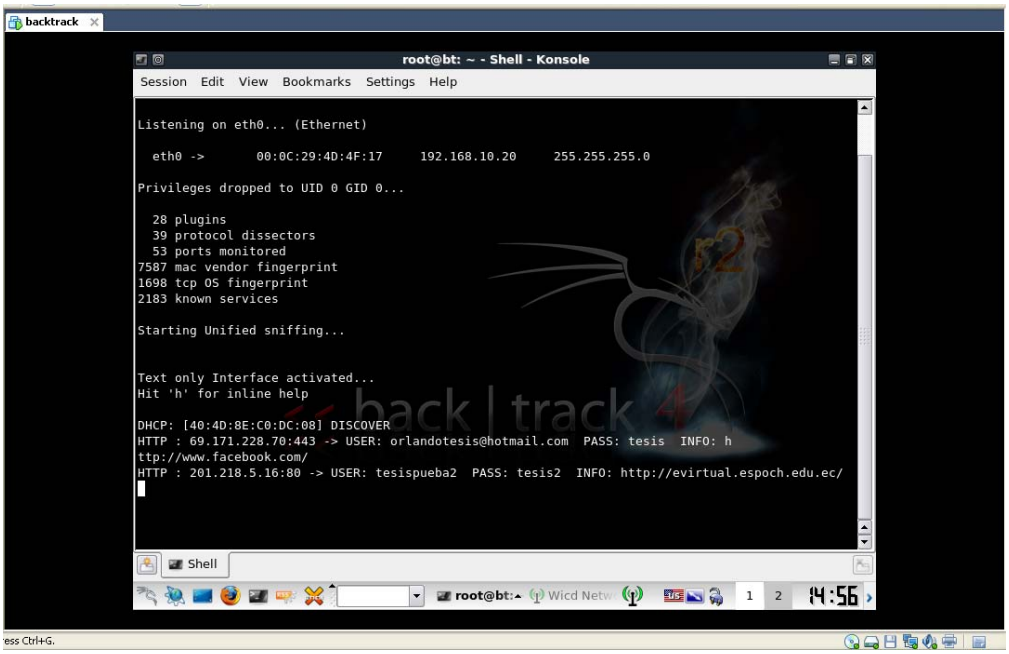


Figura IV. 40.Robo de contraseñas usando Backtrack

Confidencialidad de los datos= **0%**

- **Con la solución Implementada**

Ahora si corremos en el servidor el script del prototipo sucede lo siguiente en la pantalla de backtrack:

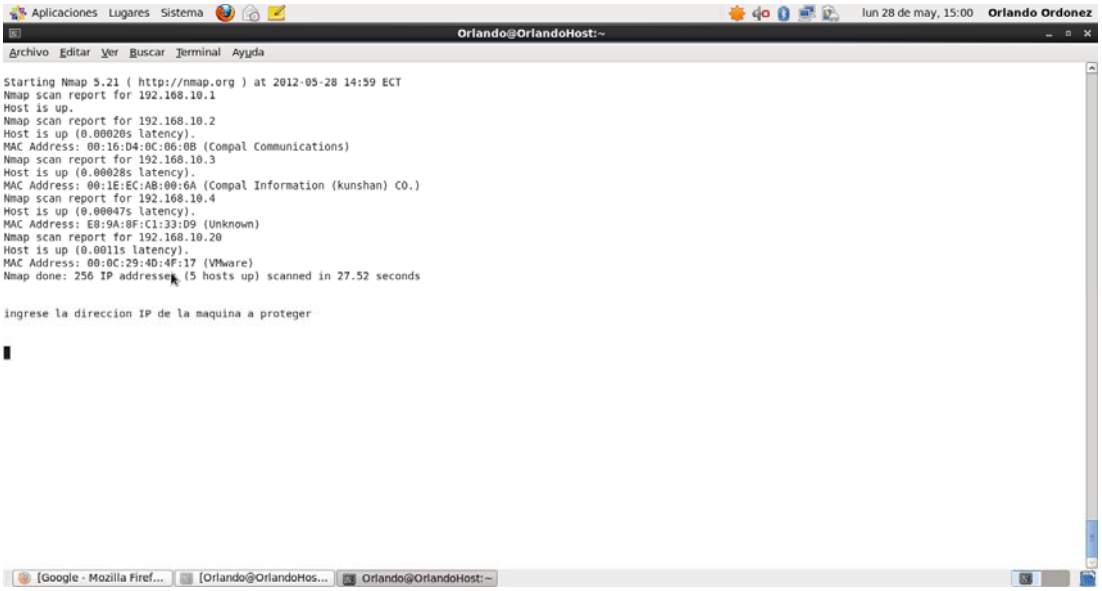


Figura IV. 41.Ejecutando la solución

Una vez corrida la solución el sistema proporciona las maquinas que se encuentran conectadas a la red y se procede asegurarlas. Una vez asegurada y si se intenta envenenar a una determinada víctima no se lo va a lograr, por lo que el intruso obtendrá en pantalla lo siguiente.

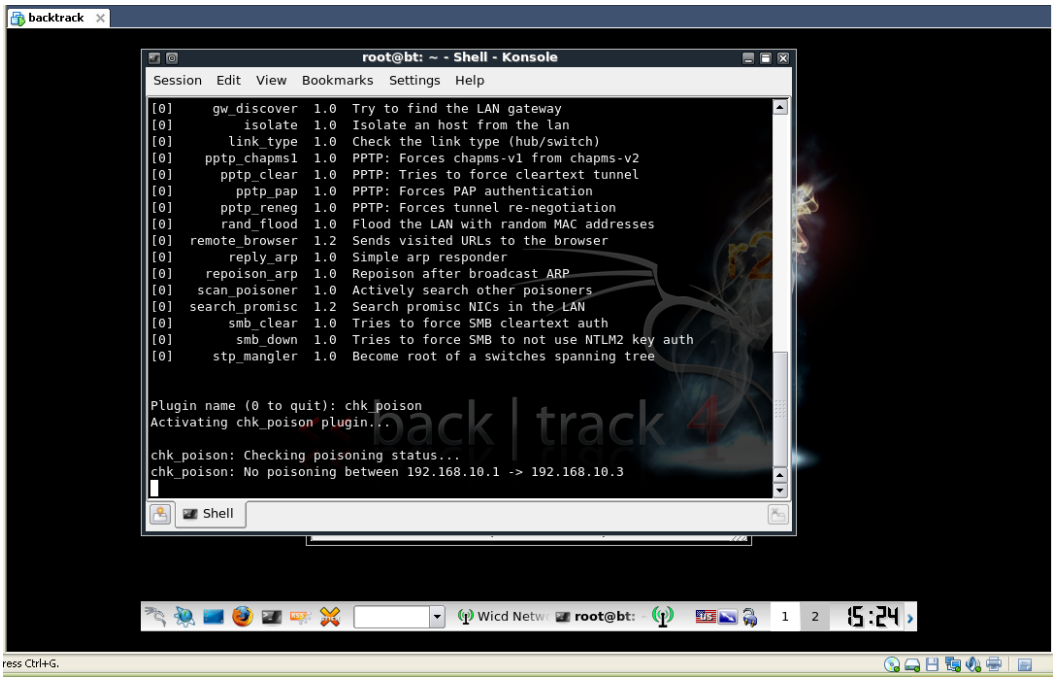


Figura IV. 42.Imposible realizar Envenenamiento

Confidencialidad de los datos= **100%**

4.3.3 Integridad de la información

Es la preservación de la modificación de información y recursos únicamente por usuarios autorizados y de la manera autorizada.

- **Sin La Solución Implementada**

  Una vez obtenido los datos de autenticación del usuario, es lógico el poder acceder a la información del mismo y modificarla afectando así a la integridad de su información.

Integridad de los datos= **0%**

- **Con La Solución Implementada**

  Mediante la implementación de la solución, como se mostro anteriormente, se pudo detener el acceso no autorizado al atacante a la información de autenticación del usuario, evitando así extraer o acceder a la información personal del usuario.

  Integridad de los datos= **100%**

4.3.4 Disponibilidad

La disponibilidad de la red se mide en el tiempo de interrupción del servicio y la pérdida de productividad de la red.

- **Sin La Solución Implementada**

Al existir un riesgo de seguridad en la red es posible ejecutar técnicas de ataque que afecten al rendimiento de la misma, como por ejemplo el ataque de denegación del servicio (DoS), impidiendo el uso de recursos de la red.

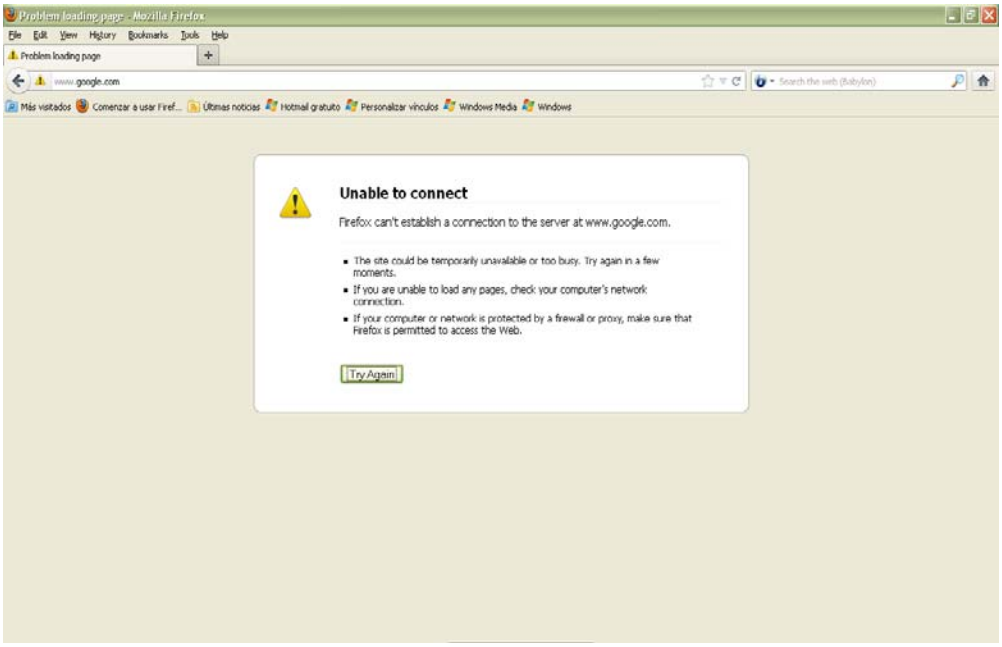


Figura IV. 43.sin la solución implementada

Disponibilidad de la red= **0%**

- **Con La Solución Implementada**

  La solución propuesta al ser implementada protege a la red de este tipo de ataques brindando disponibilidad de la red al usuario.

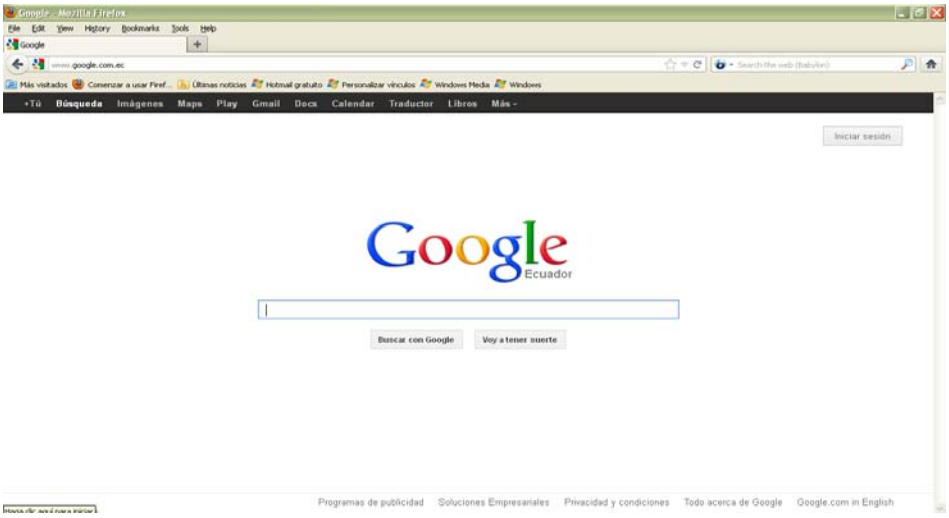


Figura IV. 44. Con la solución implementada

Disponibilidad de la Red = **100%**

4.4 Análisis de Resultados

Una vez ejecutadas las pruebas se analiza los resultados obtenidos resumiéndolo en la siguiente tabla:

	Con prototipo	**Sin prototipo**
Ping (Latencia ms)	84	184
Confidencialidad de Datos	100	0
Integridad de la información	100	0
Disponibilidad	100	0

Tabla IV. III.Análisis de resultados

4.5 Interpretación de resultados

El proceso de monitoreo de la red permite verificar el funcionamiento de la misma y los parámetros que incluye a esta. Es claro que para decir que una red está segura, esta debe proporcionar integridad total de los datos y encontrarse dentro de los parámetros que se está evaluando, donde los valores que el monitoreo arrojen estar en un nivel óptimo, de manera que no deterioren el rendimiento y menos la seguridad de la red.

Los valores recomendados establecidos para indicar que una red se encuentra en óptimas condiciones son los siguientes:

Ping (Latencia)	Confidencialidad de datos	Integridad de a información	Disponibilidad
<150 ms	100%	100%	100%

Tabla IV. IV.Interpretación de resultados

Con el monitoreo de la red se obtuvo valores que si los comparamos con los valores estándar podemos decir que se encuentra dentro de un rango aceptable de funcionamiento o de seguridad de la red.

4.6. Comprobación de los resultados

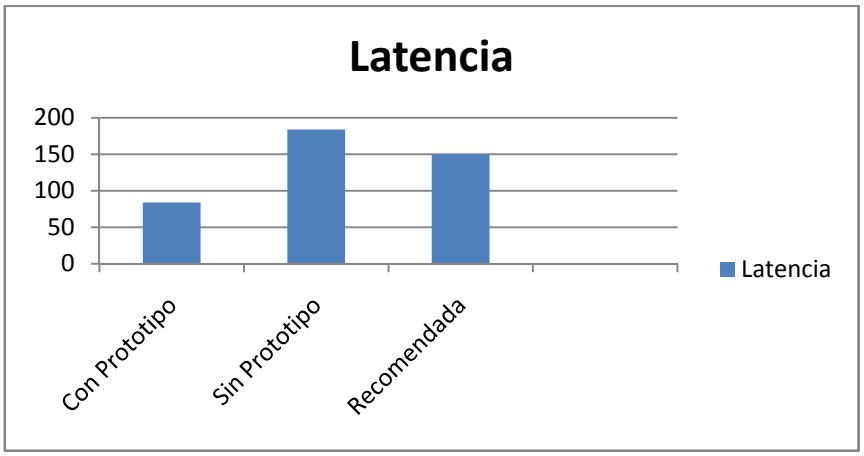


Figura IV. 45.Comprobación de la Latencia

- Fácilmente se puede apreciar que cuando el prototipo está implementado y de existir un ataque que puede ser de denegación de servicios la latencia esta dentro de los parámetros normales en los que esta debe oscilar para que el funcionamiento de la red sea óptimo, mientras que de darse esté sin que la red este protegida con el prototipo la latencia excede los límites de la normalidad y el funcionamiento de una red estable.

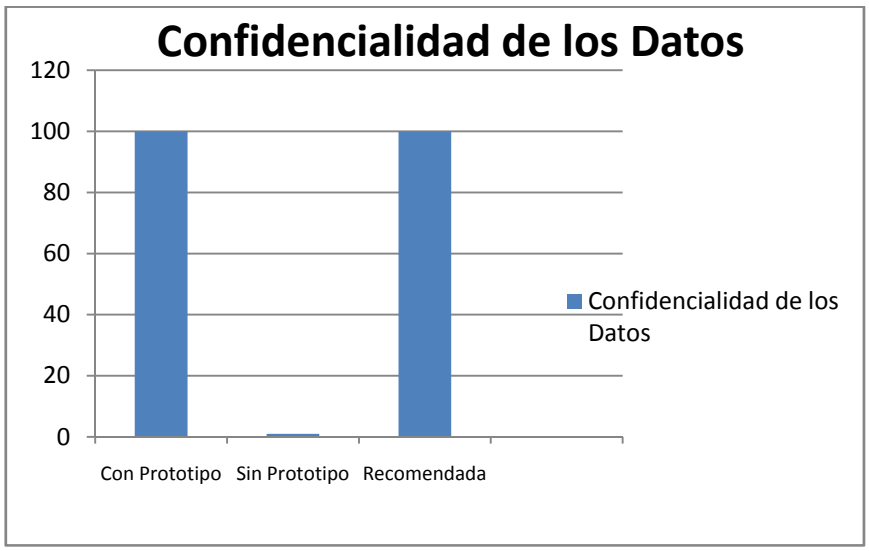


Figura IV. 46.Comprobación de la Confidencialidad de los Datos

- Se puede ver claramente que de existir un ataque a cualquier computadora de red la confidencialidad de los datos de la misma corre un gran peligro ya que el atacante puede realizar un uso mal intencionado de estos usándolos con fines no deseados para la víctima, mientras que con el prototipo implementado los datos no corren ningún riesgo de ser vistos por el atacante.

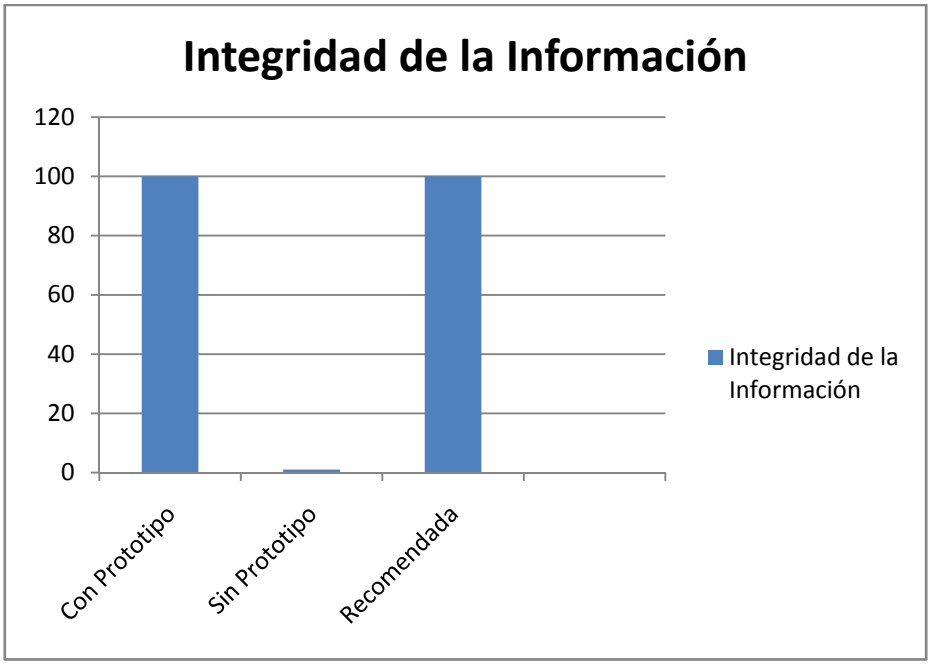


Figura IV. 47.Comprobación de la Integridad de la Información

- El gráfico anterior muestra que gracias a la implementación del prototipo los datos no corren ningún riesgo de manipulación por personas ajenas a los mismos, por lo que gracias a la solución la Integridad del Información se encuentra garantizada.

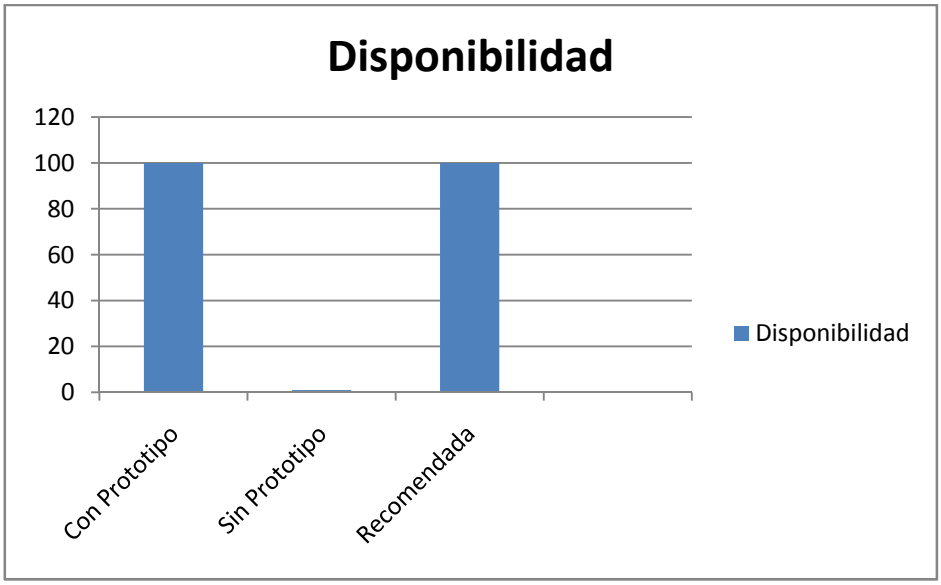


Figura IV. 48.Comprobación de la Disponibilidad de la Red

- Este último grafico nos muestra como incluso la disponibilidad de la red puede correr peligro si esta no posee la debida seguridad, el atacante al momento de suplantar la identidad de una persona que si pertenece a la red puede realizar ataques de denegación de servicio volviendo nula la disponibilidad de la red, mientras que con el prototipo instalado no lo podrá lograr.

4.7. Evaluación de la red mediante la técnica de ponderación

Se toma en cuenta la asignación de los valores en una escala de 0-10 siendo el cero un puntaje inaceptable y 10 un valor optimo, si esta dentro del rango establecido se define si cumple o no con el parámetro, se asigna los pesos a los parámetros de acuerdo a la importancia que presenta cada uno en el rendimiento de la red.

Ping

	Medio	**Recomendado**	**Cumple**
Con prototipo	**50**	**150**	**SI**
Sin Prototipo	**150**	**200**	**NO**

Tabla IV. V.Tabla evaluación de ping

Triada de la Seguridad

Parámetros	**Confidencialidad de Datos**			**Integridad de la información**			**Disponibilidad**		
	Valor	**Cumple**	**Acción**	**Valor**	**Cumple**	**Acción**	**Valor**	**Cumple**	**Acción**
Con prototipo	100	SI	No atacada	100	SI	No Alterada	100	SI	Disponible

Sin Prototipo	0	NO	Atacada	0	NO	Alterada	0	NO	DoS

Tabla IV. VI.Tabla evaluación de la Triada de la seguridad

Ponderación

		Servidor - PC			
Parámetros	**Peso**	**Con Prototipo**		**Sin Prototipo**	
		Calif	**Res**	**Calif**	**Res**
Ping (Latencia)	10%	1	10	0	0
Confidencialidad	30%	3	10	0	0
Integridad	30%	3	10	0	0
Disponibilidad	30%	3	10	0	0
		10		0	

Tabla IV. VII.Tabla de Ponderación de Datos

Mediante la técnica de ponderación se concluye que el rendimiento de la red alcanza una valoración de 10 sobre 10, equivalente al 100%, de esta manera podemos confirmar que mediante la implementación de este prototipo se pudo dar solución al gran riesgo de seguridad informática que corre una red LAN al no estar protegida de ninguna forma, y que no se necesita de muchos recursos económicos para hacerlo, comprobando así la hipótesis planteada.

CONCLUSIONES

- Mediante la implementación de este prototipo se aprendió a configurar un servidor en la distribución gratuita de LINUX denominada CentOS, mas la configuración de un IDS para una red LAN, fue de gran ayuda para implementar la solución al problema que se planteo inicialmente.

- Se verificó en nivel operativo de la red y del IDS, las pruebas se realizaron mediante el uso de un software especializado como el “Backtrack” que permite realizar auditorías en seguridad de redes.

- El prototipo demuestra que los datos de los usuarios de la red pueden estar totalmente a salvo de cualquier ataque a la red con este sistema.

- Las pruebas y el análisis de los resultados obtenidos muestran que el prototipo cumple con los requerimientos para evitar el envenenamiento ARP en una LAN.

- El uso de software libre nos permite realizar este tipo de aplicaciones sin invertir costo alguno como sucede con los software pagados.

- La seguridad e integridad de los datos dentro de la LAN garantiza la confiabilidad del proyecto realizado.

RECOMENDACIONES

- Antes de ejecutar la aplicación del prototipo, se aconseja siempre verificar que no existan problemas de tipo físico, como puede ser cables de red mal conectados o tal vez mal ponchados así como verificar que los puertos del mismo se encuentren activos, y además que la tarjeta de red externa usada en el servidor se encuentre siempre disponible.

- Al momento de ingresar los datos de las maquinas a proteger, como la dirección MAC e IP deben ser escritas correctamente en el script para que no existan conflictos en el sistema.

- Se espera que a partir de la implementación de este prototipo, se abra la posibilidad de ser implementado en otros tipos de redes distintas a las LAN con el propósito de prevenir ataques que puedan ocurrir como consecuencia de un envenenamiento ARP.

- Una LAN de preferencia siempre debe estar protegida contra intrusos y hackers para evitar daños en la información contenida en cada uno de los servidores que puedan ser vulnerables a estos tipos de ataques.

- Se recomienda capacitar al personal que va a estar a cargo de la red sobre el manejo y utilización del prototipo para mejor la seguridad en la LAN.

RESUMEN

Implementación de un prototipo mediante la utilización de software libre para evitar ataques al protocolo ARP en una red de área local.

El método deductivo permitió discernir todos los aspectos generales que intervienen y afectan en la seguridad de la red y sus factores, el método inductivo ayudó a observar parámetros específicos que miden el rendimiento de la red como la latencia, confidencialidad de la red e integridad de datos y finalmente el método analítico permitió analizar los valores con los cuales se pudo comprobar la efectividad del prototipo. Se realiza la implementación usando una PC que tiene instalada una distribución de software libre denominado CentOS versión 6, y para comprobar su efectividad otra PC que posee el software Backtrack, complementan la red 2 PC's adicionales que toman el papel de usuarios comunes.

Se detallan los resultados obtenidos al probar la solución en los distintos escenarios de ataque ARP arrojando los siguientes resultados antes de la implementación del prototipo y siendo atacada la red: latencia 184 ms, confidencialidad de los datos 0%, Integridad de los datos 0% y disponibilidad de la red 0%. Mientras que una vez implementado el prototipo: latencia 84 ms, confidencialidad de los datos 100%, Integridad de los datos 100% y disponibilidad de la red 100%.

Una vez comparados los resultados con valores establecidos como recomendados, se concluyó que el prototipo posee una efectividad del 100% en todos los parámetros considerados.

Finalmente se recomienda que este prototipo quede como ejemplo para que en un futuro sea aplicado en redes mucho más grandes y se pueda obtener los mismos resultados.

SUMMARY

Implementation of a prototype through the use of open source software in order to avoid to the ARP protocol attacks in the local area network.

The deductive method allowed to discern all general aspects that take part and affect in the network security and its factors, the inductive method helped to observe specific parameters measuring the network performance, lag time, network reliability, and data integrity and finally the analytic method allowed to analyze data which it could verify the prototype effectiveness. The implementation is carried out using a PC having installed an open source distribution software named CentOS Ver. 6, and for checking the effectiveness there is other PC installed Backtrack software, 2 additional PC's complement the network as a common users.

The results are detailed by testing in a different ARP attack scenarios giving the following results before prototype implementation and being the network attacked: lag time 184 ms, data reliability 0%, data integrity 0% and network availability 0%. While the prototype has been already installed: lag time 84 ms, data reliability 100%, data integrity 100% and network availability 100%.

Once the results are compared with established values as recommended, it is concluded that the prototype owns an effectiveness of 100% in all parameters considered.

Finally it is recommended this prototype be a pattern in the future applying in networks much bigger with the same results.

Key words: implementation, prototype, ARP protocol, CentOS.

GLOSARIO

Iptables.- Herramienta que permite aplicar reglas para crear un firewall. Lo interesante es que forma parte del kernel de linux (a partir del 2.4).

Live CD.- Traducido en ocasiones como **CD vivo** o **CD autónomo**, es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de archivos.

Plugin.- Programa que puede anexarse a otro para aumentar sus funcionalidades (generalmente sin afectar otras funciones ni afectar la aplicación principal). No se trata de un parche ni de una actualización, es un módulo aparte que se incluye opcionalmente en una aplicación.

GNU/LINUX.- Es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado **Linux**, que es usado con herramientas de sistema GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (**L**icencia **P**ública **G**eneral de GNU, en inglés: **G**eneral **P**ublic **L**icense) y otra serie de licencias libres.

Protocolo TCP / IP.- Es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa. TCP / IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en el ARPANET una red de área extensa del departamento de defensa.

Modelo TCP / IP.- Un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda

comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando como los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Existen protocolos para los diferentes tipos de servicios de comunicación entre equipos.

Ettercap.- Un interceptor/sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing.

Sniffer.- Es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

Exploit.- Es una pieza de software, o una secuencia de comandos con el fin de causar un error o un fallo en alguna aplicación, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado). Con frecuencia, esto incluye cosas tales como la toma de control de un sistema de cómputo o permitir la escalada de privilegios o un ataque de denegación de servicio. El fin del Exploit puede ser violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.

ANEXOS

ANEXO 1

Script para correr la solución.

```
#!/bin/bash
clear
echo "          ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO"
echo
echo
echo
echo "                                  TESIS DE GRADO"
echo
echo
echo
echo "                                  ORLANDO ORDONEZ"
echo
echo
echo "    LAS REDES QUE SE ENCUENTRAN CONECTADAS A SU PC SON:"
echo
echo
echo 1 > /proc/sys/net/ipv4/ip_forward
ifconfig eth0 192.168.10.1/24
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
route -n
echo
# while
echo
"./tesis" 48L, 875C
```

BIBLIOGRAFÍA

1. **Philip R.,** Securing Wireless Networks from ARP Cache Poisoning. In partial Fulfillment of the Requirements for the Degree Master of Computer Science., EE.UU - San Jose State., 2007., Pp. 3 8 - 9 - 10 -14
   2011-10-28
2. **ANTICAP**
   http://www.antifork.org/viewcvs/trunk/anticap
   2011-12-12
3. **ARP GUARD**
   https://www.arp-guard.com/
   2011-11-15
4. **ARP SPOOFING**
   http://es.wikipedia.org/wiki/ARP_Spoofing
   2011-09-30
5. **ATAQUE MAN-IN-THE-MIDDLE**
   http://es.wikipedia.org/wiki/Ataque_Man-in-the-middle

2012-02-14

6. **BACKTRACK**

http://es.wikipedia.org/wiki/BackTrack

2012-04-20

7. **CENTOS 6**

http://www.centos.org/

2012-04-02

8. **EBTABLES**

http://ebtables.sourceforge.net

2012-01-07

9. **ELEMENTOS DEL IDS**

http://es.scribd.com/doc/68731192/30/Decodificador

2012-03-22

10. **ETTERCAP**

http://www.alevsk.com/2010/07/ettercap-potente-herramienta-de-auditorias-lan/

2012-05-01

11. **REDES DE COMPUTADORAS**

http://es.wikipedia.org/wiki/Red_de_computadoras

2011-06-30

12. **REDES DE DATOS**

http://es.wikitel.info/wiki/Redes_de_datos

2012-02-13

13. **RIESGOS INFORMÁTICOS**

http://www.basc-costarica.com/documentos/riesgosinformatica.pdf

2012-03-30

14. **SEGURIDAD DE LA INFORMACIÓN**

http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

2011-07-15

15. **SECURE NEIGHBOR DISCOVERY PROTOCOL**

http://en.wikipedia.org/wiki/Secure_Neighbor_Discovery

2011-08-14

16. SNORT.ORG

http://www.snort.org/

2012-02-02