UNIVERSITAT POLITÈCNICA DE VALÈNCIA

SEGURIDAD EN REDES A NIVEL DE CAPA 2

ANDRÉS GUSTAVO MUÑOZ DÁVILA
INGENIERÍA TÉCNICA EN TELECOMUNICACIONES
ESP. TELEMÁTICA

JULIO ,2011
DIRECTOR DE PROYECTO: CARLOS SASTRE
DEPARTAMENTO: LABDISCA

TABLA DE CONTENIDO

INDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

2. OBJETIVOS

- Tener un conocimiento acerca de los conceptos de VLAN, MAC, STP y ARP.
- Conocer los tipos de ataques que se pueden presentar en las VLAN, MAC, STP y ARP.
- manejar diferentes herramientas de ataque.
- Conocer las diferentes características de seguridad de los Dispositivos Cisco

1. INTRODUCCIÓN

El modelo OSI (figura 1.1) se pensó para que cada capa opére independientemente de las demas. Esto quiere decir que cada capa puede ser comprometida sin que las otras lo noten (figura 1.2).

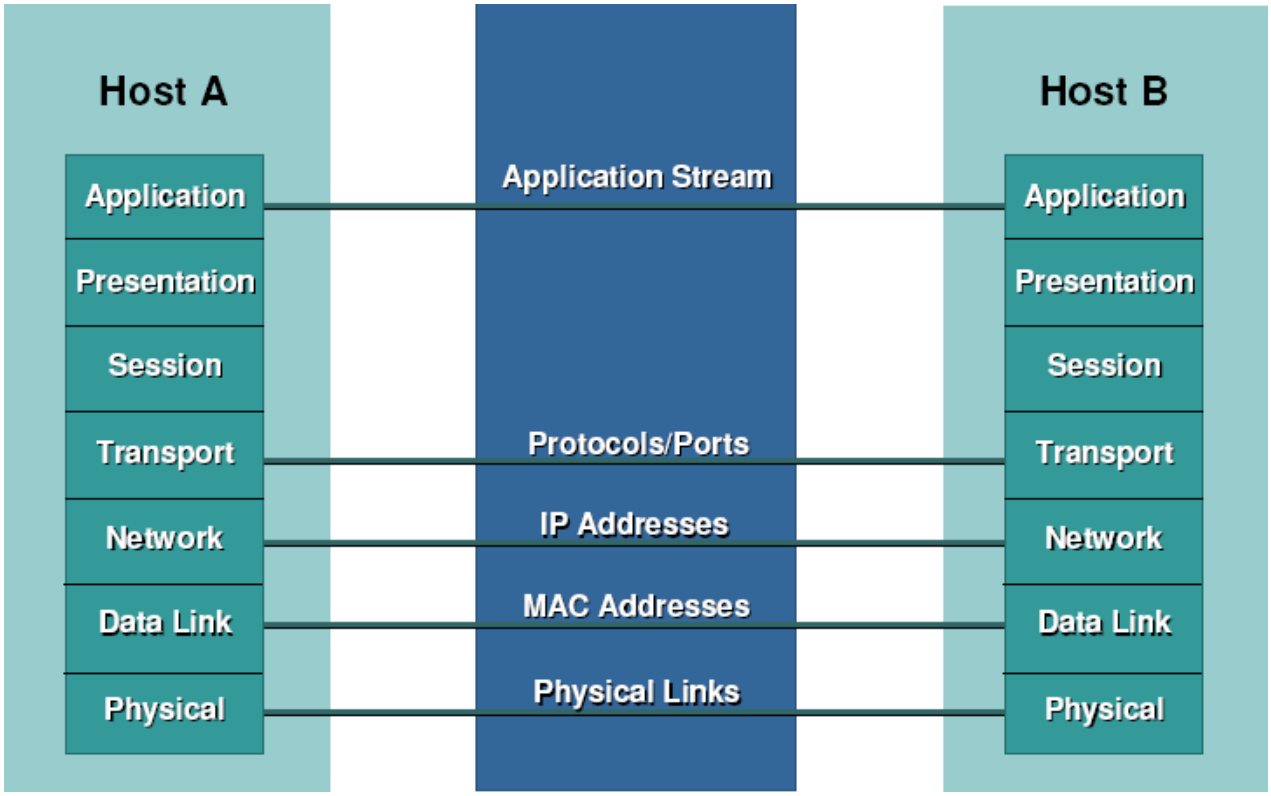


Figura 1.1: Modelo OSI

- Según el FBI el 80% de los ataques provienen al interior de la organización
- El 99% de los puertos (o bocas) de las redes LAN corporativas están "desprotegidos". Es decir, cualquiera puede conectarse a ellos.
- La mayoría de las empresas está desplegando redes inhalámbricas (aunque no lo sepan).
- Las herramientas diseñadas para simplificar el trabajo de los administradores de red perjudican seriamente la seguridad de la red corporativa.

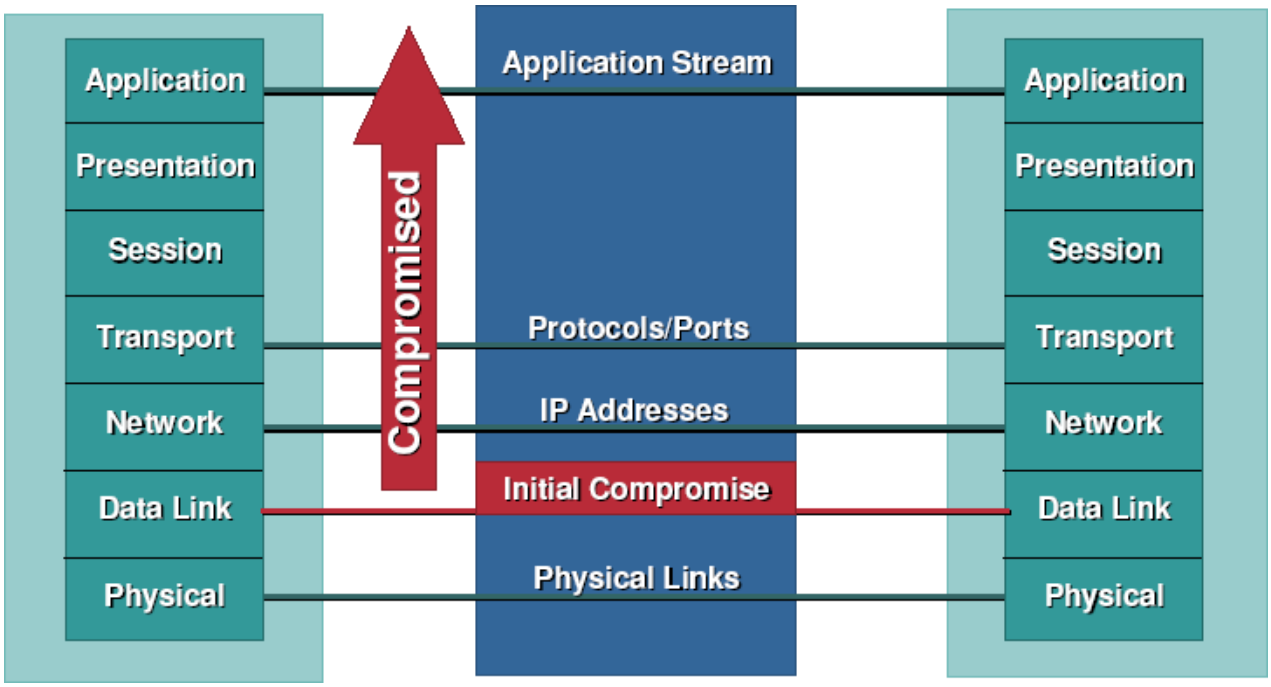


Figura 1.2: Capas Comprometidas: Modelo OSI

1.1. Mitos De La Capa 2

- Las direcciones MAC no pueden ser falsificadas.
- Un switch no permite hacer sniffing.
- Las VLAN's están separadas unas de las otras .

1.2. El Modelo OSI

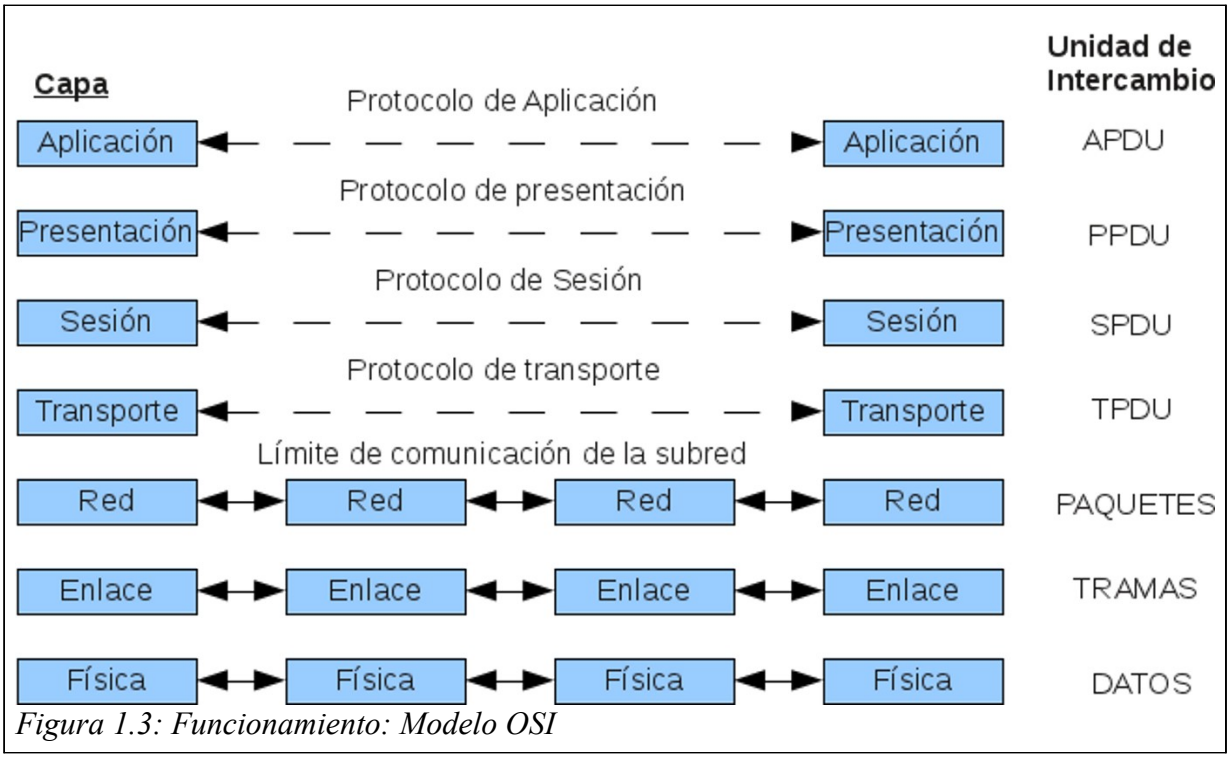


Figura 1.3: Funcionamiento: Modelo OSI

El modelo OSI nace como una solución a la incompatibilidad de las redes en la década del 80; este modelado por capaz o niveles permite que las comunicaciones se organicen en una "pila" de protocolos y que cada capa sea independiente de las demás.

El funcionamiento sería algo así: (Figura 1.3)

Desde la capa de aplicación se genera un "paquete"(PDU) como se muestra en (Figura 1.4). A este se le va agregando información en cada capa necesaria para la comunicación entre cada una de ellas sobre las diferentes máquinas:

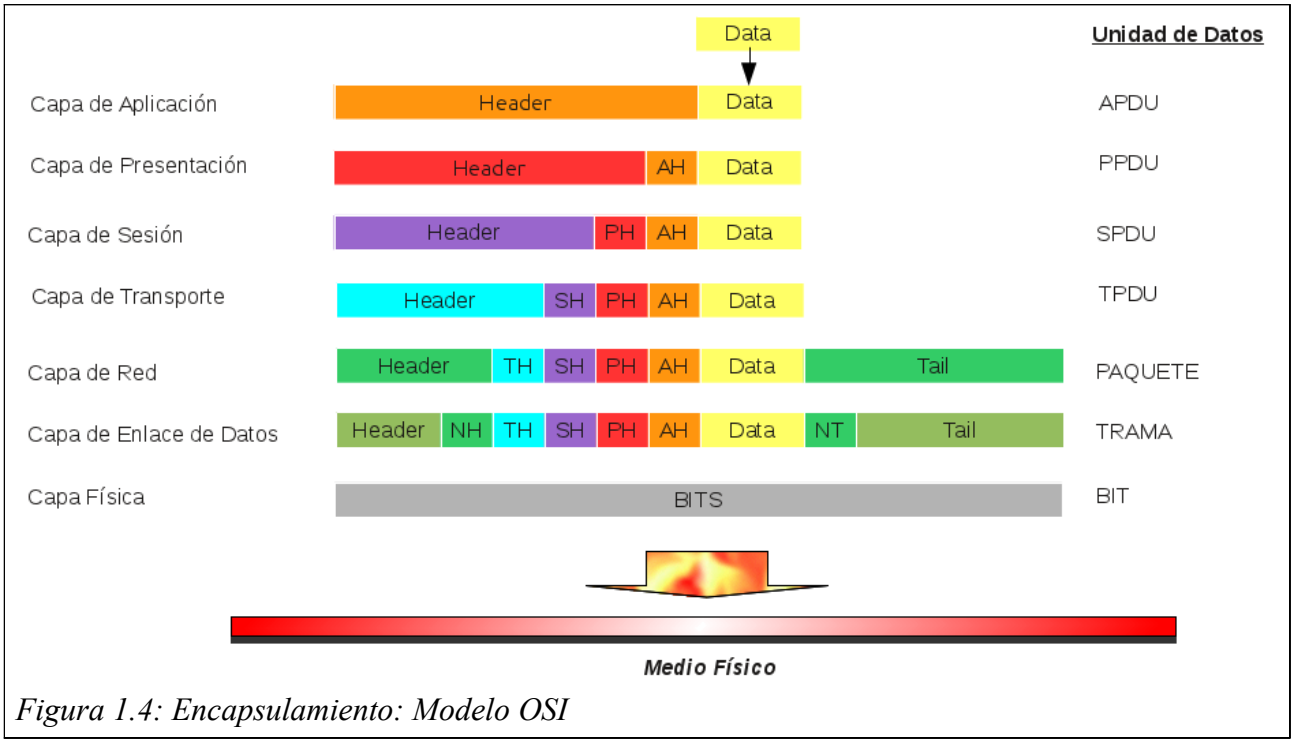


Figura 1.4: Encapsulamiento: Modelo OSI

El resultado obtenido en la capa de enlace de datos es la trama que enviaremos al medio físico para transmitirla. Como podemos ver en la (Figura 1.3) , la trama antes de llegar a la máquina destino va a pasar por switchs (capa 2 aunque existen switchs de capa 3) y routers (capa 3). En los routers la trama se va "abriendo", por decirlo de alguna manera y se obtiene la información que se necesita en cada nivel, ya sea la MAC (capa 2) en caso de los switchs o en los routers la MAC y la IP (capa 3) para poder hacer la redirección de las tramas por los caminos correctos. Una vez que se obtienen dichos datos, se vuelve a armar el paquete y a partir de los resultados obtenidos continúa su camino por la red hasta llegar a la máquina destino.

Bueno eso es OSI y así funciona, aclaremos que el modelo en sí mismo no es considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, por eso es que suele hablarse de modelo de referencia.

2. ATAQUES

2.1. Ataques Basados En MAC Y ARP

Para comprender el funcionamiento de este tipo de ataques hablaremos un poco del protocolo ARP. ARP son las siglas en inglés de *Address Resolution Protocol* (Protocolo de resolución de direcciones). Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast (MAC = xx xx xx xx xx xx) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto sólo funciona si todas las máquinas lo soportan. ARP está documentado en el RFC[1] 826

El protocolo RARP realiza la operación inversa.

En Ethernet, la capa de enlace trabaja con direcciones físicas. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas).Para realizar ésta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC. ARP se utiliza en 4 casos referentes a la comunicación entre 2 hosts:

- Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.
- Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
- Cuando un router necesita enviar un paquete a un host a través de otro router.
- Cuando un router necesita enviar un paquete a un host de la misma red.

2.1.1. Tablas ARP.

La filosofía es la misma que tendríamos para localizar al señor "X" entre 150 personas: preguntar por su nombre a todo el mundo, y el señor "X" nos responderá. Así, cuando a "A" le llegue un mensaje con dirección origen IP y no tenga esa dirección en su tabla ARP, enviará su trama ARP a la dirección broadcast (física), con la IP de la que quiere conocer su dirección física. Entonces, el equipo cuya dirección IP coincida con la preguntada, responderá a "A" enviándole su dirección física. En este momento "A" ya puede agregar la entrada de esa IP a su tabla ARP. Las entradas de la tabla se borran cada cierto tiempo, ya que las direcciones físicas de la red pueden cambiar (Ej: si se estropea una tarjeta de red y hay que sustituirla, o simplemente algún usuario de la red cambia de dirección IP).

2.1.1.1. FUNCIONAMIENTO EN EL CASO 1.

Si A quiere enviar una trama a la dirección IP de B (misma red), mirará su tabla ARP para poner en la trama la dirección destino física correspondiente a la IP de B. De esta forma, cuando les llegue a todos la trama, no tendrán que deshacerla para comprobar si el

1 *De las siglas en inglés: Request For Comments*

mensaje es para ellos, sino que se hace con la dirección física.

2.1.1.2. FUNCIONAMIENTO EN EL CASO 2.

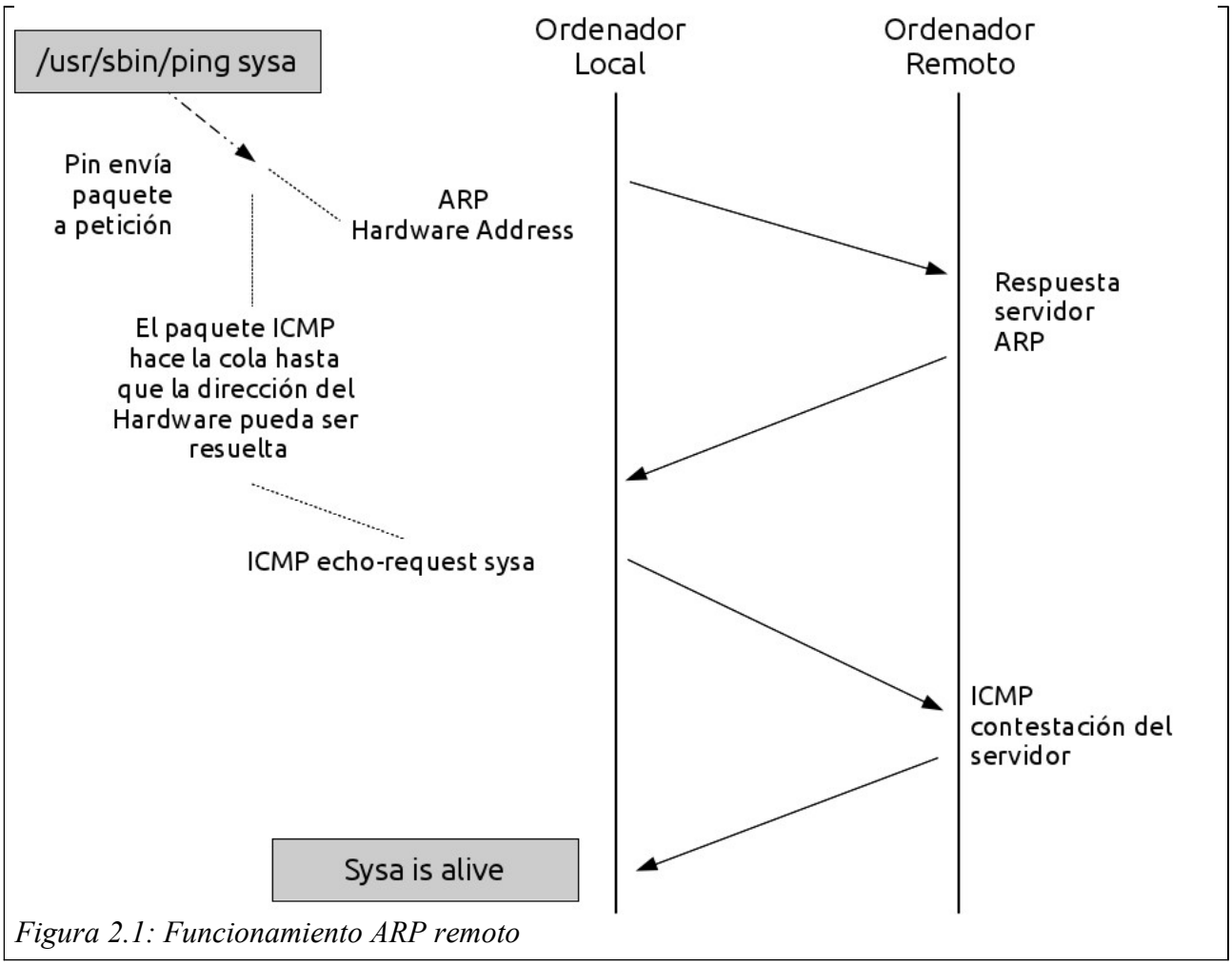


Figura 2.1: Funcionamiento ARP remoto

(Figura 2.1) Si A quiere enviar un mensaje a C (un nodo que no esté en la misma red), el mensaje deberá salir de la red. Así, A envía la trama a la dirección física de salida del router. Esta dirección física la obtendrá a partir de la IP del router, utilizando la tabla ARP. Si esta entrada no está en la tabla, mandará un mensaje ARP a esa IP (llegará a todos), para que le conteste indicándole su dirección física.

Una vez en el router, éste consultará su tabla de encaminamiento, obteniendo el próximo nodo (salto) para llegar al destino, y saca el mensaje por la interfaz correspondiente. Esto se repite por todos los nodos, hasta llegar al último router, que es el que comparte el medio con el host destino. Aquí el proceso cambia: la interfaz del router tendrá que averiguar la dirección física de la IP destino que le ha llegado. Lo hace mirando su tabla ARP, y en caso de no existir la entrada correspondiente a la IP, la obtiene realizando una multidifusión.

Pare el ataque basado en MAC y ARP encontramos 3 tipos:

- CAM Table Overflow.
- ARP Spoofing
- Ataques que emplean ARP Spoofing.

2.1.2. CAM Table Overflow.

El ataque se basa en la limitación del hardware del switch para mantener la tabla que relaciona las MAC con los puertos, dicha tabla se denomina CAM[2] Obviamente las tablas no son infinitas y cuando una llega a su tope un switch comienza a trabajar como un HUB, es decir que todo paquete que recibe el switch si la MAC destino no se encuentra en la tabla y ésta se encuentra llena, manda el paquete por todos sus puertos. Esto nos permitiría capturar todo el tráfico con un sniffer obviamente capturaríamos las tramas que se dirigen a MAC's que no se encuentren en la tabla, pero como sabemos que las asignaciones son temporales, lo que se hace es mandar las MAC's falsas en intervalos de tiempo lo suficientemente chicos como para que se llene la tabla con MAC's falsas y cuando las verdaderas caen por vencimiento de tiempo, estos espacios se llenan con más MAC's falsas; y así lograríamos mantener el ataque. (Figura 2.2)

Bien para producir este *overflow* lo que se hace es enviar muchas tramas con direcciones MAC distintas a cualquier puerto del switch hasta que en un momento empecemos a

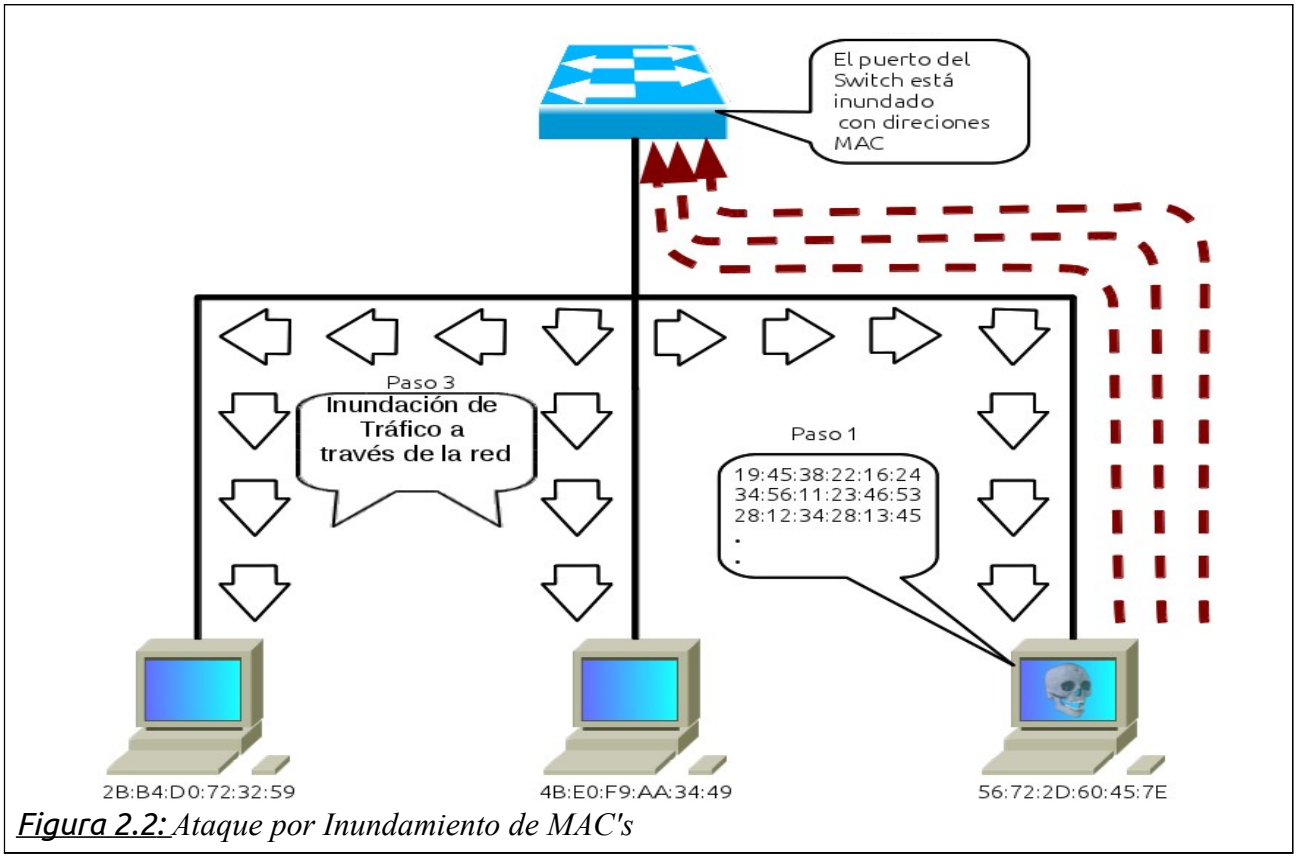


Figura 2.2: Ataque por Inundamiento de MAC's

recibir las tramas que se dirigen a otras máquinas (esto lo detectamos con el sniffer).

2 . *Siglas en Ingles: Content Addressable Memory*

Obviamente este tipo de cosas producen inestabilidad sobre la red, no sería raro que se encuentren con un DOS (*Denial of service*) en vez de empezar a recibir paquetes. Existe una herramienta para producir este tipo de ataques denominada macof, es parte del paquete Dsniff (GNU/Linux) y el codigo esta escrito en perl. Para utilizarlo es suficiente con instalar el paquete d*sniff* y ejecutar *macof*.
Existen medidas contra este tipo de ataques, algunas de ellas son asignar a los puertos del switch un limite de MAC's a asignar, y en el caso que esa cantidad se supere producir el bloqueo de dicho puerto o directamente utilizando asignaciones estáticas de MAC a los puertos (que entre mas grande la red require mucho trabajo).

2.1.3. ARP Spoofing

También conocido como ARP Poisoning o ARP Poison Routing. Para este ataque debemos tener claro el funcionamiento del protocolo ARP para cambiar la MAC. Para poder comunicarnos en un ámbito local necesitamos la MAC, para ello mandamos un pedido ARP que nos la retornara y luego se almacenara en la tabla durante cierto intervalo de tiempo, ahora bien también existen los GARP[3] estos son paquetes que contienen la MAC y la IP de un host y se mandan en broadcast a toda la red para que todos los hosts existentes en ella actualicen su caché ARP Importante¡ (todos los que esten configurados como dinámicos y acepten estos pedidos). Estos paquetes no generan una respuesta de parte de las máquinas que los reciben pero cuando una máquina lo recibe lo asigna a su tabla.

Al ser mensajes broadcast no están diseñados para proporcionar ninguna validación de identificación en la transacción, por ende falsificar la información que estos paquetes llevan sería muy sencillo, y manteniendo el envió de estos paquetes en intervalos de tiempos lo suficientemente cortos como para que las caches no borren las entradas, conseguiríamos generar conexiones virtuales distintas a las conexiones reales.

2.1.3.1. ¿COMO SERIA EL ATAQUE?

Supongan que 2 máquinas dentro de la red se quieren conectar,la *máquina1* con una *IP Y* y *MAC X, la máquina2* con una *IP Z y MAC M*, si estas quisieran comunicarse deberían utilizar un pedido para la MAC a menos que las tengan en sus tablas, pero ¿Que pasa si estuvieran "mal" cargadas? Suponga además que esta la máquina del atacante con *IP A* y *MAC B* y manda un paquete GARP en broadcast con la siguiente información (*IP Z, MAC B*) :O, este paquete le indicaría a la máquina1 que para llegar a la *IP Z* (de la *máquina 2*) debe mandar el paquete a la *MAC B* (máquina del atacante). De ahora en más todo paquete de máquina1 a máquina2 pasara por la máquina atacante, y si este último redireccionara dichos paquetes a la máquina2 generaríamos una conexión con nuestra máquina atacante en el medio y pasando por ella toda la comunicación (!*Excelente día para un sniffer*¡) bueno a este tipo de ataque se lo denomina *Switch Port Stealing*. Existe un ataque bastante similar denominado MITM[4] pero con un detalle más importante... que pasaría si mandamos el mismo GARP desde la máquina atacante y decimos que para la IP de gateway del router de la red la MAC es B :O, de ahora en más todo paquete de cualquier máquina en la red que quiera obtener información de una IP fuera de la red,

3 . *(Gratuitous ARP o ARP announcement)*
4 *Siglas en Ingles: Man in the Middle*

pasarían por la máquina atacante.(Otro Excelente día para sniffear). Para estos ataques existe Ettercap (*Figura 2.3).*

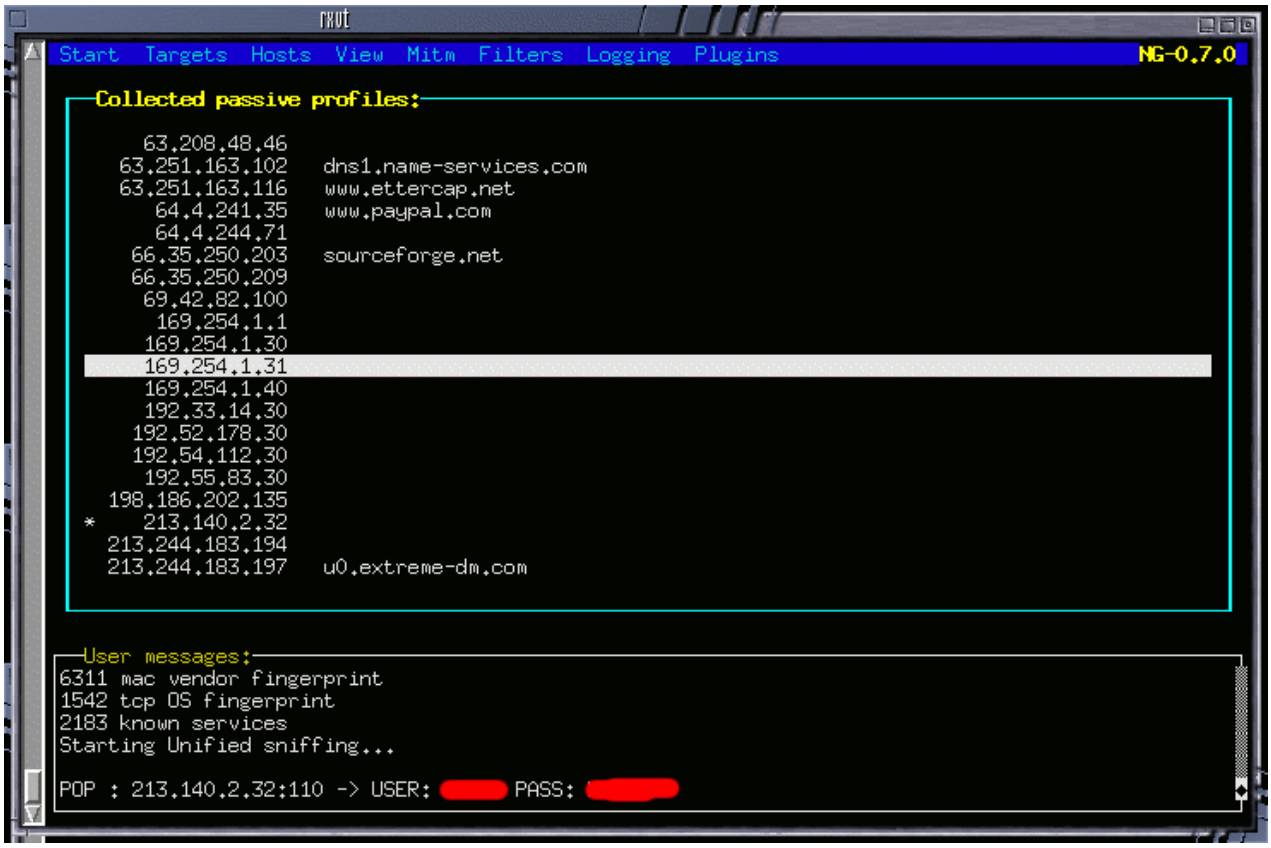


Figura 2.3: Ettercap

Y así podemos jugar con las MAC particulares como la de broadcast(FF:FF:FF:FF:FF), ¿Que pasaría si en vez de mandar la MAC de la máquina atacante (B), decimos que la IP de gateway se dirige a la MAC de broadcast? todos los paquetes de todas las máquinas que quieran salir de la red serán enviados a todas las máquinas de la red.

2.1.4. Ataques Que Emplean ARP Spoofing.

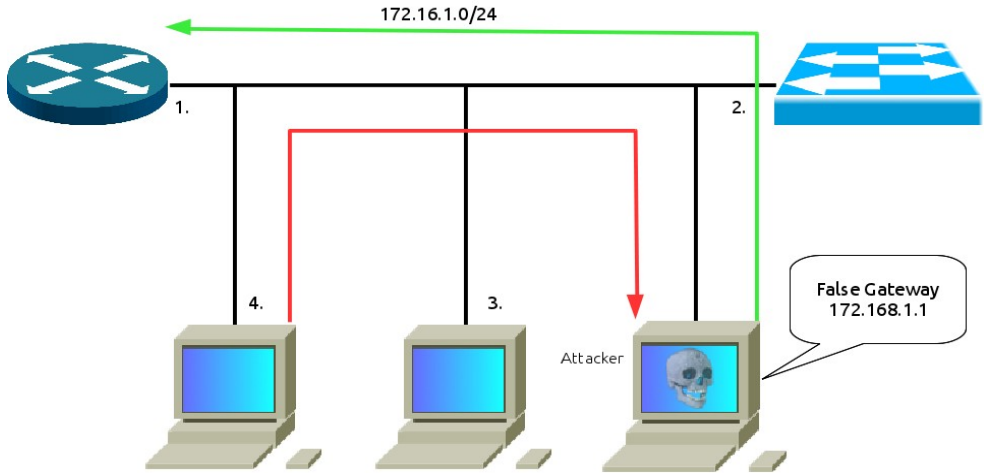


Figura 2.4: ARP Spoofing

Dentro de este tenemos 2:

- DoS (Denial of Service) l(a figura 2.5 nos muestra un ejemplo de este ataque)

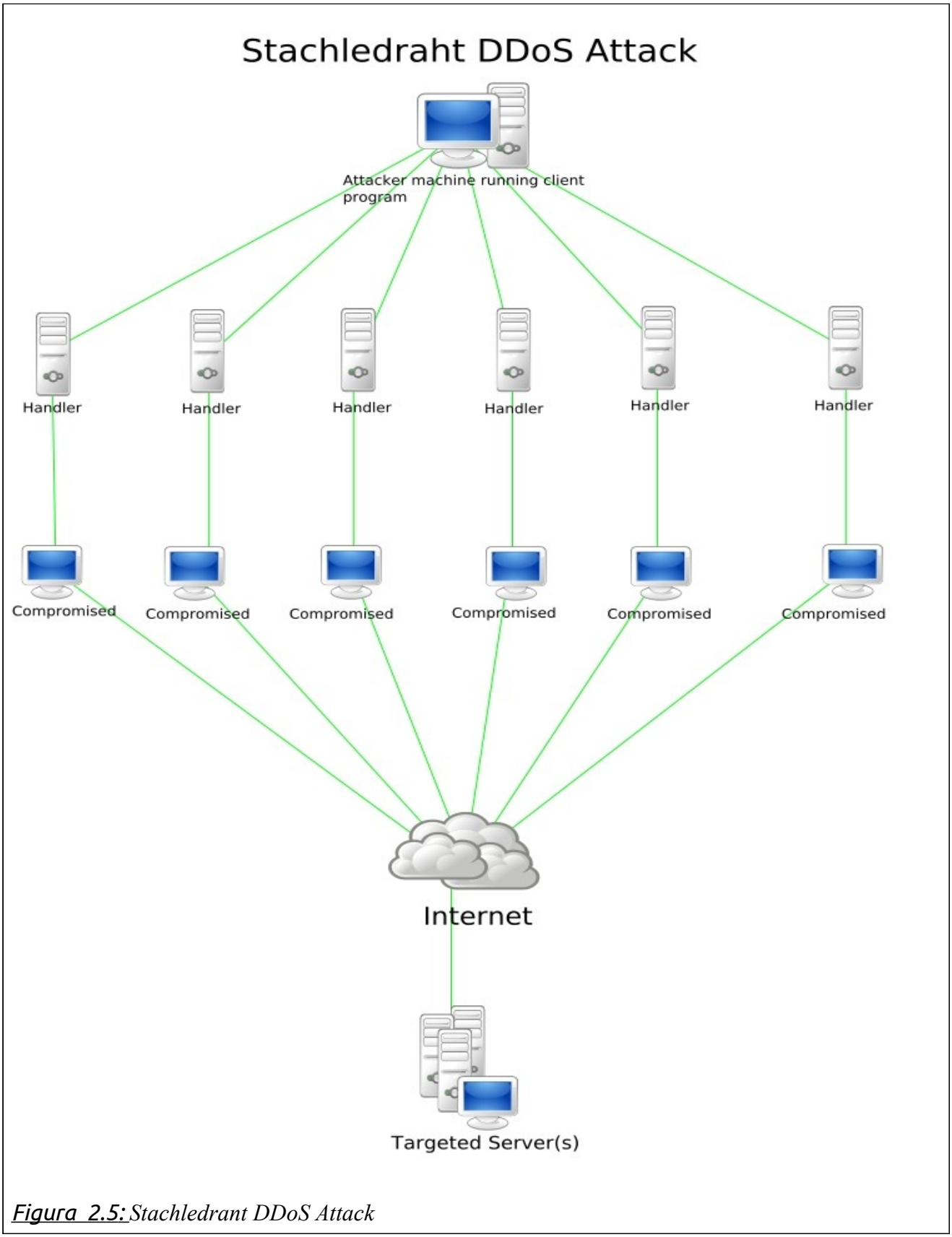


Figura 2.5: Stachledrant DDoS Attack

- Hijacking

2.1.4.1. DOS (DENIAL OF SERVICE)

Bueno este es bastante sencillo, sigue siendo el mismo formato de los anteriores pero la diferencia es que quiere dejar sin servicio a alguna máquina de la red. Lo que hacemos para lograrlo es asignar en el paquete GARP[5] a una IP existente en la red una MAC inexistente por ende los paquetes se descartaran y esa máquina nunca va a recibir una respuesta de ningún host en la red.

En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS[6], es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no dé abasto a la cantidad de usuarios. Esta

técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DdoS *Figura 2.7* (de las siglas en inglés Distributed Denial of Service) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

La forma más común de realizar un DDoS a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz.

En ocasiones, esta herramienta ha sido utilizada como un notable método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y perjudicar los servicios que desempeña. Un administrador de redes puede así conocer la capacidad real de cada máquina.

2.1.4.1.1. Métodos de ataque.

Un ataque de "Denegación de servicio" impide el uso legítimo de los usuarios al usar un servicio de red. El ataque se puede dar de muchas formas. Pero todas tienen algo en común: utilizan el protocolo TCP/IP para conseguir su propósito.

Un ataque DoS puede ser perpetrado en un numero de formas. Aunque básicamente consisten en :

- Consumo de recursos computacionales, tales como ancho de banda, espacio de disco,

5 *Gratuitous ARP o ARP announcement Gratuitous*
6 *de las siglas en inglés Denial of Service*

o tiempo de procesador.
- Alteración de informacion de configuración, tales como información de rutas de encaminamiento.
- Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset).
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.

2.1.4.1.2. Inundación SYN (SYN Flood)

2.1.4.1.2.1. Principios de TCP/IP

Cuando una máquina se comunica mediante TCP/IP[7] con otra, envía una serie de datos junto a la petición real. Estos datos forman la cabecera de la solicitud. Dentro de la cabecera se encuentran unas señalizaciones llamadas Flags (banderas). Estas señalizaciones (banderas) permiten iniciar una conexión, cerrarla, indicar que una solicitud es urgente, reiniciar una conexión, etc. Las banderas se incluyen tanto en la solicitud (cliente), como en la respuesta (servidor).

Para aclararlo, veamos cómo es un intercambio estándar TCP/IP:

1. Establecer Conexión: El cliente envía una Flag SYN, si el servidor acepta la conexión, este, debería responderle con un SYN/ACK luego el cliente debería responder con una Flag ACK.

   1-Cliente ----------SYN------> 2 Servidor
   4-Cliente <-----SYN/ACK---- 3 Servidor
   5-Cliente ----------ACK------> 6 Servidor
   ---

2. Resetear Conexión: Al haber algún error o perdida de paquetes de envio se establece envio de Flags RST:

   1-Cliente ---------Reset------> 2-servidor
   4-Cliente <----Reset/ACK----3-Servidor
   5-Cliente ----------ACK-------- 6-Servidor

La inundación SYN[8] envía un flujo de paquetes TCP/SYN (varias peticiones con Flags SYN en la cabecera), muchas veces con la dirección de origen falsificada. Cada uno de los paquetes recibidos es tratado por el destino como una petición de conexión, causando que el servidor intente establecer una conexión al responder con un paquete TCP/SYN-ACK y esperando el paquete de respuesta TCP/ACK (Parte del proceso de establecimiento de conexión TCP de 3 vías). Sin embargo, debido a que la dirección de origen es falsa o la dirección IP real no ha solicitado la conexión, nunca llega la

7 *TCP/IP*
8 *De las siglas en Ingles SYN*

respuesta. Estos intentos de conexión consumen recursos en el servidor y limitan el número de conexiones que se pueden hacer, reduciendo la disponibilidad del servidor para responder peticiones legítimas de conexión.

2.1.4.1.2.2. SYN cookies

provee un mecanismo de proteccion contra Inundación SYN, eliminando la reserva de recursos en el host destino, para una conexión en momento de su gestión inicial.

2.1.4.1.3. Inundación ICMP (ICMP Flood)

Es una técnica DoS que pretende agotar el ancho de banda de la víctima. Consiste en enviar de forma continuada un número elevado de paquetes ICMP Echo request (ping) de tamaño considerable a la víctima, de forma que esta ha de responder con paquetes ICMP Echo reply (pong) lo que supone una sobrecarga tanto en la red como en el sistema de la víctima.
Dependiendo de la relación entre capacidad de procesamiento de la víctima y el atacante, el grado de sobrecarga varía, es decir, si un atacante tiene una capacidad mucho mayor, la víctima no puede manejar el tráfico generado.

2.1.4.1.4. SMURF

Existe una variante a ICMP Flood denominado Ataque Smurf que amplifica considerablemente los efectos de un ataque ICMP.

Existen tres partes en un Ataque Smurf: El atacante, el intermediario y la víctima (comproba-remos que el intermediario también puede ser víctima).

En el ataque Smurf, el atacante dirige paquetes ICMP tipo "echo request" (ping) a una direc-ción IP de broadcast, usando como dirección IP origen, la dirección de la víctima (Spoofing). Se espera que los equipos conectados respondan a la petición, usando Echo reply, a la má-quina origen (víctima).

Se dice que el efecto es amplificado, debido a que la cantidad de respuestas obtenidas, co-rresponde a la cantidad de equipos en la red que puedan responder. Todas estas respuestas son dirigidas a la víctima intentando colapsar sus recursos de red.
Como se dijo anteriormente, los intermediarios también sufren los mismos problemas que las propias víctimas.

2.1.4.1.5. Inundación UDP (UDP Flood)

Básicamente este ataque consiste en generar grandes cantidades de paquetes UDP contra la víctima elegida. Debido a la naturaleza sin conexión del protocolo UDP, este tipo de ataques suele venir acompañado de IP Spoofing.
Es usual dirigir este ataque contra máquinas que ejecutan el servicio Echo, de forma que se generan mensajes Echo de un elevado tamaño.

2.1.4.2. HIJACKING

Hijacking [9] hace referencia a toda técnica ilegal que lleve consigo el adueñarse o robar algo (generalmente información) por parte de un atacante. Es por tanto un concepto muy abierto y que puede aplicarse a varios ámbitos, de esta manera podemos encontramos con el secuestro de conexiones de red, sesiones de terminal, servicios, modems y un largo etcétera en cuanto a servicios informáticos se refiere.

2.1.4.2.1. Ejemplos de Hijacking

IP hijakers: secuestro de una conexión TCP/IP por ejemplo durante una sesión Telnet permitiendo a un atacante inyectar comandos o realizar un DoS durante dicha sesión.
Page hijacking: secuestro de página web. Hace referencia a las modificaciones que un atacante realiza sobre una página web, normalmente haciendo uso de algún bug de seguridad del servidor o de programación del sitio web, también es conocido como defacement o desfiguración.
Reverse domain hijacking o Domain hijacking: secuestro de dominio
Session hijacking: secuestro de sesión
Browser hijacking: (Secuestro de navegadores en español). Se llama así al efecto de apropiación que realizan algunos spyware sobre el navegador web lanzando popups, modificando la página de inicio, modificando la página de búsqueda predeterminada etc. Es utilizado por un tipo de software malware el cual altera la configuración interna de los navegadores de internet de un ordenador. El termino "secuestro" hace referencia a que éstas modificaciones se hacen sin el permiso y el conocimiento del usuario. Algunos de éstos son fáciles de eliminar del sistema, mientras que otros son extremadamente complicados de eliminar y revertir sus cambios.
Home Page Browser hijacking: secuestro de la página de inicio del navegador. Esto sucede cuando la página de inicio, en la que navegamos es cambiada por otra a interés del secuestrador. Generalmente son páginas en las que nos invita a usar los servicios de la página para que nuestro equipo esté seguro y funcione correctamente. No cabe decir que es a cambio de un pago y que el origen del error y mal funcionamiento del equipo es debido a nuestro secuestrador
Modem hijacking: secuestro del Modem. Esta expresión es en ocasiones utilizada para referirse a la estafa de los famosos dialers que tanta guerra dieron en su día (antes del auge del ADSL) y que configuran sin el consentimiento del usuario nuevas conexiones a números de cobro extraordinario.
Thread hijacking: secuestro de un "tema" dentro de un foro de discusión de internet. Este termino hace referencia a la situación que ocurre cuando dentro de un tema de discusión en un foro alguien intenta dirigir el hilo de la conversación hacia asuntos que no tienen nada que ver con el tema inicial. Esto puede realizarse de manera intencionada para irritar al autor del tema o bien producirse de manera natural y no intencionada generalmente por usuarios sin mucho conocimiento en el asunto a tratar o que desconocen la dinámica de comportamiento de los foros.

2.2. Ataques Basados En VLAN

9 *significa "secuestro" en inglés y en el ámbito informático*

Para entender este tipo de ataque vamos explicar que es una VLAN y como trabaja. Es un método para crear redes lógicamente independientes dentro de una misma red fícica Una 'VLAN' consiste en una red de ordenadores que se comportan como si estuviesenconectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

2.2.1. Protocolos Y Diseño.

El protocolo de etiquetado IEEE 802.1Q domina el mundo de las VLANs. Antes de su introducción existían varios protocolos propietarios, como el ISL (Inter-Switch Link) de Cisco, una variante del IEEE 802.1Q, y el VLT (Virtual LAN Trunk) de 3Com.

Los primeros diseñadoras de redes enfrentaron el problema del tamaño de los dominios de colision (Hubs) esto se logró controlar a través de la introducción de los switch o conmutadores pero a su vez se introdujo el problema del aumento del tamaño de los dominios de difusión y una de las formas más eficientes para manejarlo fue la introducción de las VLANs. Las VLANs también pueden servir para restringir el acceso a recursos de red con independencia de la topología física de ésta, si bien la robustez de este método es discutible al ser el salto de VLAN (VLAN hopping) un método común de evitar tales medidas de seguridad.

Las VLANs funcionan en el nivel 2 (enlace de datos) del modelo OSI. Sin embargo, los administradores suelen configurar las VLANs como correspondencia directa de una red o subred IP, lo que les da apariencia de funcionar en el nivel 3 (red).

En el contexto de las VLANs, el término trunk (‘troncal’) designa una conexión de red que transporta múltiples VLANs identificadas por etiquetas (o tags) insertadas en sus paquetes. Dichos trunks deben operar entre tagged ports (‘puertos etiquetados’) de dispositivos con soporte de VLANs, por lo que a menúdo son enlaces conmutador a conmutador o conmutador a enrutador más que enlaces a nodos. (Para mayor confusión, el término trunk también se usa para lo que Cisco denomina «canales»;. Un enrutador (conmutador de nivel 3) funciona como columna vertebral para el tráfico de red transmitido entre diferentes VLANs.

En los dispositivos Cisco, VTP (VLAN Trunking Protocol) permite definir dominios de VLAN, lo que facilita las tareas administrativas. VTP (Cisco) también permite «podar», lo que significa dirigir tráfico VLAN específico sólo a los conmutadores que tienen puertos en la VLAN destino.

2.2.2. Ejemplo De Definición De VLAN

Imaginemos que en nuestra empresa tenemos una LAN corporativa con un rango de

direcciones IP tipo 172.16.1.XXX. Se da el caso de que tenemos asignadas las casi 255 direcciones que como máximo nos permite el mismo y además notamos cierta saturación en la red. Una fácil solución a este problema sería crear unas cuantas VLAN por medio de un switch o conmutador de nivel 3.

Podemos asignar una VLAN a cada departamento de la empresa, así también controlamos que cada uno sea independiente (o no) del resto:

VLAN1: Contabilidad. Direcciones 172.16.2.XXX

VLAN2: Compras. Direcciones 172.16.3.XXX

VLAN3: Distribución. Direcciones 172.16.4.XXX

.

De esta forma liberamos direcciones de nuestra red origen 172.16.1.XXX pasándolas a las distintas VLAN que hemos creado. Gracias al switch de nivel 3 podremos gestionar la visibilidad entre las distintas VLAN y notaremos una mejora en el rendimiento de la red ya que las difusiones o broadcast de cada VLAN sólo llegarán a los equipos conectados a la misma.

2.2.3. Gestión De La Pertenencia A Una VLAN

Las dos aproximaciones más habituales para la asignación de miembros de una VLAN son las siguientes: VLANes estáticas y VLANes dinámicas

Las VLANes estáticas también se denominan VLANes basadas en el puerto. Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un switch o conmutador a dicha VLAN. Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto. Si el usuario cambia de puerto de entrada y necesita acceder a la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el switch.

En las VLANes dinámicas, la asignación se realiza mediante paquetes de software tales como el CiscoWorks 2000. Con el VMPS (acrónimo en inglés de VLAN Policy Server o Servidor de Directivas de la VLAN), el administrador de la red puede asignar los puertos que pertenecen a una VLAN de manera automática basándose en información tal como la dirección MAC del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo. En este procedimiento, el dispositivo que accede a la red, hace una consulta a la base de datos de miembros de la VLAN. Se puede consultar el software FreeNAC para ver un ejemplo de implementación de un servidor VMPS.

2.2.4. VLAN Basadas En El Puerto De Conexión

Con las VLANes con pertenencia basada en el puerto de conexión del switch, el puerto asignado a la VLAN es independiente del usuario o dispositivo conectado en el puerto. Esto significa que todos los usuarios que se conectan al puerto serán miembros de la

misma VLAN. Habitualmente es el administrador de la red el que realiza las asignaciones a la VLAN. Después de que un puerto ha sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3.

El dispositivo que se conecta a un puerto, posiblemente no tenga conocimiento de la existencia de la VLAN a la que pertenece dicho puerto. El dispositivo simplemente sabe que es miembro de una sub-red y que puede ser capaz de hablar con otros miembros de la sub-red simplemente enviando información al segmento cableado. El switch es responsable de identificar que la información viene de una VLAN determinada y de asegurarse de que esa información llega a todos los demás miembros de la VLAN. El switch también se asegura de que el resto de puertos que no están en dicha VLAN no reciben dicha información.

Este planteamiento es sencillo, rápido y fácil de administrar, dado que no hay complejas tablas en las que mirar para configurar la segmentación de la VLAN. Si la asociación de puerto-a-VLAN se hace con un ASIC (acrónimo en inglés de Application-Specific Integrated Circuit o Circuito integrado para una aplicación específica), el rendimiento es muy bueno. Un ASIC permite el mapeo de puerto-a-VLAN sea hecho a nivel hardware.

2.2.4.1. TIPOS DE ATAQUE

Dentro de este tipo de ataque encontramos 4 tipos:

- Dynamic Trunking protocol.
- VLAN Hopping Attack.
- Double Encapsulated VLAN Hopping Attack.
- VLAN Trunking Protocol.

2.2.4.2. DYNAMIC TRUNKING PROTOCOL.

Para hablar sobre este ataque hablaremos primero que es y como funciona el protocolo.

DTP[10] es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

Dicho protocolo puede establecer los puertos ethernet en cinco modos diferentes de trabajo: AUTO, ON, OFF, DESIRABLE y NON-NEGOTIATE.

2.2.4.2.1. Modos de trabajo de los puertos

- dynamic auto — Es el modo por defecto en switches Catalyst 2960 de Cisco. El puerto aguardará pasivamente la indicación del otro extremo del enlace para pasar a modo troncal. Para ello envía periódicamente tramas DTP al puerto en el otro lado del enlace indicando que es capaz de establecer un enlace troncal. Esto no quiere decir

10 *De las siglas en inglés: Dynamic Trunking Protocol*

que lo solicita, sino que sólo lo informa. Si el puerto remoto está configurado en modo on o dynamic desirable se establece el enlace troncal correctamente. Sin embargo, si los dos extremos estan en modo dynamic auto no se establecerá el enlace como troncal, sino como acceso, lo que probablemente implique configuración adicional.

- on — Suele ser el modo por defecto. Fuerza al enlace a permanecer siempre en modo troncal, aún si el otro extremo no está de acuerdo.

- off — Fuerza al enlace a permanecer siempre en modo de acceso, aún si el otro extremo no está de acuerdo.

- dynamic desirable — Es el modo por defecto en switches Catalyst 2950 de Cisco. En este modo el puerto activamente intenta convertir el enlace en un enlace t roncal. De este modo, si en el otro extremo encuentra un puerto en modo on, dynamic auto o dynamic desirable pasará a operar en modo troncal.

- nonegotiate — Fuerza siempre al puerto a permanecer en modo troncal, pero no envía tramas DTP. Los vecinos deberán establecer el modo troncal en el enlace de forma manual.

2.2.4.2.2. Configuración de DTP

DTP[11] se habilita automáticamente en un puerto del switch cuando se configura un modo de trunking adecuado en dicho puerto. Para ello el administrador debe ejecutar el comando switchport mode adecuado al configurar el puerto: switchport mode {access | trunk | dynamic auto | dynamic desirable}. Con el comando switchport nonegotiate se desactiva DTP.

Su función es gestionar de forma dinámica la configuración del enlace troncal al conectar dos switches, introduciendo los comandos del IOS (sistema operativo de los switches y routers Cisco) en la configuración del dispositivo (running-config) de forma automática sin que el administrador intervenga.

Esto implica que si estamos configurando un puerto de un switch Cisco para DTP, el puerto del otro lado del enlace también debe tener DTP habilitado para que el enlace quede configurado correctamente.

La combinación de los modos asignados a los puertos define cuál va a ser el estado final del enlace asociado a éstos:

- o bien 'access', es decir, pasarán las tramas de una única VLAN y no necesitaremos etiquetarlas.
- o bien 'trunking', es decir, pasarán las tramas de todas las VLAN permitidas etiquetándolas adecuadamente (ISL o 802.1Q).

La *Tabla 2.1* describe las combinaciones de modos y el estado final del puerto al que se llega, asumiendo que ambos lados tienen DTP habilitado:

11 *De las siglas en inglés: Dynamic Trunking Protocol*

Table 2.1: Modos y combinaciones de los puertos DTP

Remoto \ ***Puerto local*** \	**Dynamic Auto**	**Dynamic Desirable**	**Trunk**	**Access**
Dynamic Auto	access	trunk	trunk	access
Dynamic Desirable	trunk	trunk	trunk	access
Trunk	trunk	trunk	trunk	**fallo**
Access	access	access	**fallo**	access

Este protocolo es una ayuda que facilita la vida del administrador de la red. Los switches no necesitan DTP para establecer enlaces troncales, y algunos switches y routers Cisco no soportan DTP.

2.2.4.2.3. Puertos TRUNK.

Los puertos trunk por defecto tienen acceso a todas las VLANs. Se los emplea para transmitir tráfico de múltiples VLANs a través del mismo enlace físico (generalmente empleado para conectar switches). La encapsulación puede ser IEEE 802.1Q o ISL[12]. *Figura 2.4*

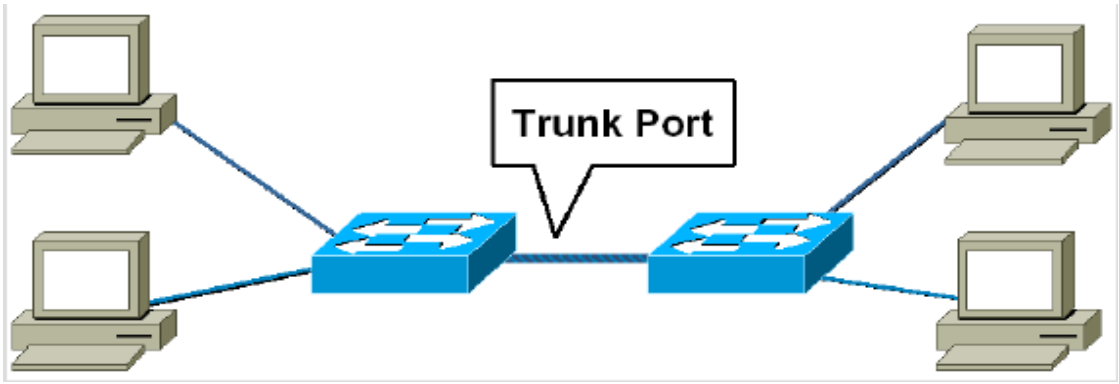


Figura 2.6: Puertos Trunk

2.2.4.2.4. Principales caracteristicas empleadas en el ataque.

- Automatiza la configuración de los trunk 802.1Q/ISL.
- Sincroniza el modo de trunking en los extremos.
- Hace innecesaria la intervención administrativa enambos extremos.
- El estado de DTP en un puerto trunk puede ser “Auto”, “On”, “Off”, “Desirable”, o “Non-Negotiate”. Por default en la mayoría de los switchs es “Auto”.

Para este ataque podemos usar el frame work para el ataque en capa 2 llamado *Yersinia.*

2.2.5. VLAN Hopping Attack.

12

VLAN Hopping (*virtual local area network hopping*) es un método de atacar a los recursos en red en una VLAN. El concepto básico detrás de todos los ataques de salto de VLAN es para un host atacante en una VLAN para tener acceso al tráfico en otras VLAN que normalmente no serían accesibles. Hay dos métodos principales VLAN Hopping: switch spoofing y doble etiquetado.

2.2.5.1. ATAQUE SWITCH SPOOFING.

En un ataque de switch spoofing, un host atacante que sea capaz de hablar de etiquetado y protocolos Trunking utilizados en el mantenimiento de una VLAN que imita un conmutador trunking. El Tráfico para varias VLAN es entonces accesible a la máquina atacante.

2.2.5.2. DOUBLE TAGGING ATTACK.

En un ataque de etiquetado doble, un host atacante antepone dos etiquetas VLAN a paquetes que transmite. El primer encabezado (que corresponde a la VLAN que el atacante es realmente un miembro de) es despojado por un primer conmutador que encuentre el paquete, y entonces el paquete se envía. El segundo, falso, el encabezado es entonces visible para el segundo conmutador que se encuentra con el paquete. Este falso encabezado VLAN indica que el paquete está destinado para un host en un segundo, VLAN de destino. El paquete es enviado al host de destino como si se tratara de tráfico en la capa 2. Mediante este método, la máquina atacante puede pasar por alto medidas de seguridad de la capa 3 que se utilizan para aislar lógicamente los host de los demás.

Como un ejemplo de un ataque de doble etiquetado, considere un servidor web seguro en una VLAN llamada VLAN1. Los hosts de la VLAN1 permite el acceso al servidor web, los host de fuera de la VLAN están bloqueados por los filtros de la capa 3. Un host atacante en una VLAN separada, llamada VLAN2, crea un paquete especialmente creado para atacar el servidor web. Se coloca una encabezado de etiqueta del el paquete como perteneciente a VLAN2 en la parte superior de otro encabezado de etiqueta del paquete como perteneciente a la VLAN1. Cuando el paquete es enviado, el interruptor de VLAN2 ve la cabecera VLAN2 y lo elimina, y envía el paquete. El interruptor VLAN2 espera que el paquete será tratado como un paquete del estándar de TCP por el conmutador en VLAN1. Sin embargo, cuando el paquete llega a VLAN1, el interruptor ve una etiqueta que indica que el paquete es parte de la VLAN1, y así evita la capa 3, tratándolo como un paquetes en la red capa de 2 en la misma VLAN lógica. El paquete por lo tanto llega al servidor de destino como si fuera enviado desde otro host en VLAN1, haciendo caso omiso de cualquier filtrado de capa 3 que podría estar en su lugar.

2.2.5.3. ¿COMO SE PRODUCE ESTE ATAQUE? (*FIGURA 2.9*)

- Un equipo puede hacerse pasar como un switch con IEEE802.1Q/ISL y DTP, o bien se puede emplear un switch.

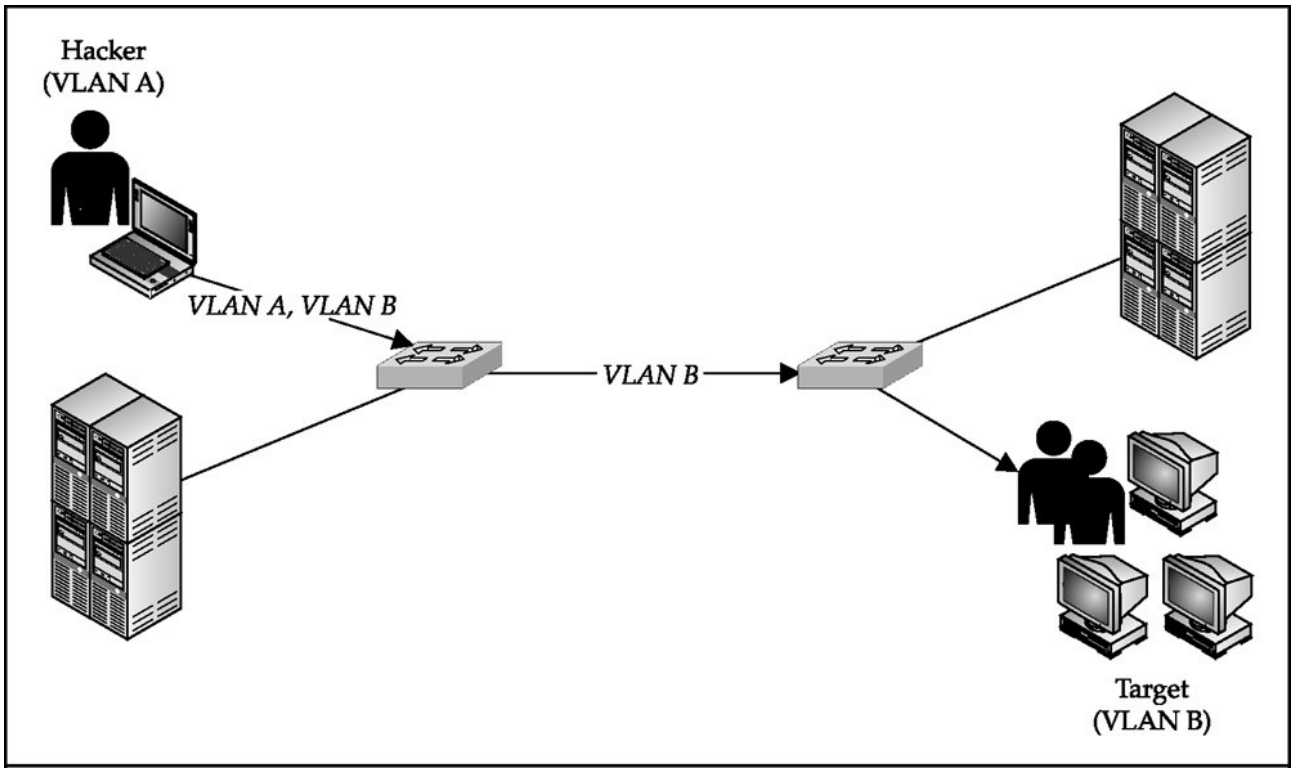


Figura 2.7: Ataque de doble etiquetado

- El equipo se vuelve miembro de todas las VLAN.
- Requiere que el puerto este configurado con trunking automático.

2.2.6. Ataque De VLAN De Doble-Encapsulamiento 802.1Q/Nested .

Mientras interno a un Switch, los números de VLAN y la identificación se llevan en un formato especial extendido que permite la ruta de transmisión para mantener el aislamiento de VLAN de extremo a extremo sin ninguna pérdida de información. En cambio, fuera de un conmutador, las normas de etiquetado son dictados por las normas ISL o 802.1Q.

ISL es una tecnología propietaria de Cisco y en cierto sentido es una forma compacta de la cabecera del paquete ampliada utilizados en el interior del dispositivo: desde que todos los paquetes adquieran una etiqueta, no hay riesgo de pérdida de identidad y por lo tanto de las vulnerabilidades de seguridad. Por otra parte, la IEEE que definió 802.1Q decidió que, debido a la compatibilidad anterior era conveniente apoyar la bien llamada VLAN nativa, es decir, una VLAN que no se asocia explícitamente a cualquier etiqueta en un enlace 802.1Q . Esta VLAN es implícitamente usada para todo el tráfico sin etiquetar recibido en un puerto 802.1Q capaz de recibirlo.

Esta capacidad es deseable porque permite a los puertos 802.1Q capaces de hablar con los viejos puertos 802,3 directamente mediante el envío y recepción de tráfico sin etiquetar. Sin embargo, en los demás casos, puede ser muy perjudicial porque los paquetes asociados con la VLAN nativa pierden sus etiquetas, por ejemplo, su aplicación de identidad, así como su clase de servicio (802.1p bits) cuando se transmiten a través de un enlace 802.1Q.

Por estas razones exclusivas la pérdida de medios de identificación y la pérdida de la clasificación, el uso de la VLAN nativa debe ser evitado. Hay una razón más sutil, sin embargo. Si bien interno a un conmutadorr, los números de VLAN y la identificación se llevan en un formato especial extendido que permite la ruta transmisión para mantener el aislamiento de VLAN de extremo a extremo sin ninguna pérdida de información. En cambio, en las afueras de un interruptor, las normas de etiquetado son dictados por las normas ISL o 802.1Q.

La (*figura 2.6*) describe como trabaja este ataque.

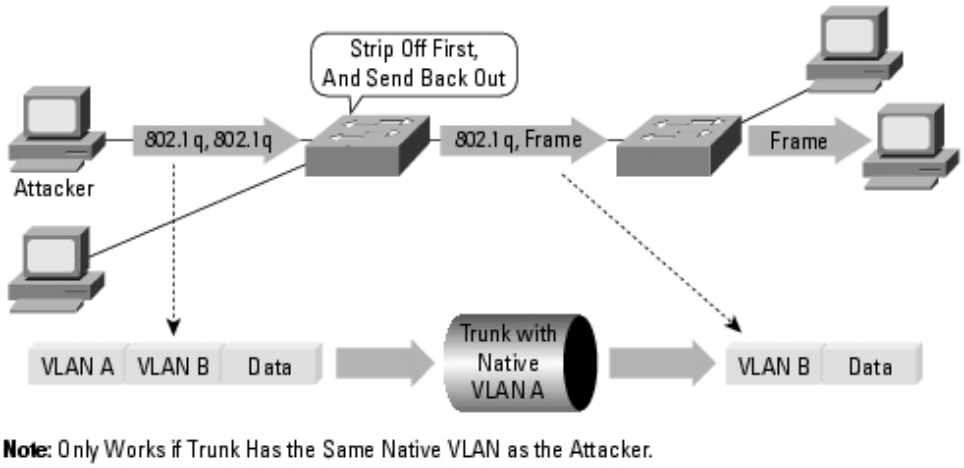


Figura 2.8: Ataque de VLAN de Doble-Encapsulamiento 802.1Q/Nested

- Se envian una trama 802.1Q de la VLAN de lavíctima dentro de otra trama 802.1Q de nuestra VLAN.
- Los switchs realizan un solo nivel de desencapsulado.
- Solo permite tráfico en una sola dirección.
- Sólo funciona si la VLAN nativa del trunk es la misma a la que pertenece el atacante.
- Funciona aunque el puerto del atacante tenga desactivado el trunking.

2.2.7. VLAN Trunking Protocol

VTP son las siglas de *VLAN Trunking Protocol,* un protocolo usado para configurar y administrar VLANs en equipos Cisco. VTP opera en 3 modos distintos: - Cliente - Servidor - Transparente

Los administradores de red solo pueden cambiar la configuración de VLANs en modo Servidor. Después de que se realiza algún cambio, estos son distribuidos a todos los demás dispositivos en el dominio VTP a través de los enlaces que permiten el Trunk. Los dispositivos que operan en modo transparente no aplican las configuraciones VLAN que reciben, ni envían las suyas a otros dispositivos, sin embargo los dispositivos en modo transparente que usan la versión 2 del protocolo VTP enviarán la información que

reciban (publicaciones VTP) a otros dispositivos a los que estén conectados, actualmente (año 2009) dichas publicaciones se envían cada 5 minutos. Los dispositivos que operen en modo cliente, automáticamente aplicarán la configuración que reciban del dominio VTP, en el modo cliente NO se podrán crear VLAN, sino que sólo podrá aplicar la información que reciba de las publicaciones VTP.

Las configuraciones VTP en una red son controladas por un número de revisión. Si el número de revisión de una actualización recibida por un switch en modo cliente o servidor es más alto que la revisión anterior, entonces se aplicará la nueva configuración. De lo contrario se ignoran los cambios recibidos. Cuando se añaden nuevos dispositivos a un dominio VTP, se debe resetear los números de revisión de todo el dominio VTP para evitar conflictos. Se recomienda mucho cuidado al usar VTP cuando haya cambios de topología ya sean lógicos o físicos.

Realmente no es necesario resetear todos los números de revisión del dominio. Sólo hay que asegurarse de que los switches nuevos que se agregen al dominio VTP tengan números de revisión más bajos que los que están configurados en la red. Si no fuese así, bastaría con eliminar el nombre del dominio del switch que se agrega. Esa operación vuelve a poner a cero su contador de revisión.

El VTP permite a un administrador de red configurar un switch de modo que propagará las configuraciones de la VLAN hacia los otros switches en la red. El switch se puede configurar en la función de servidor del VTP o de cliente del VTP. El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN, denominada vlan.dat.

El VTP permite al administrador de red realizar cambios en un switch que está configurado como servidor del VTP. Básicamente, el servidor del VTP distribuye y sincroniza la información de la VLAN a los switches habilitados por el VTP a través de la red conmutada, lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias en las configuraciones. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN denominada vlan.dat. Para que dos equipos que utilizan VTP puedan compartir información sobre VLAN, es necesario que pertenezcan al mismo dominio.

2.2.8. Seguridad VTP

VTP puede operar sin autenticación, en cuyo caso resulta fácil para un atacante falsificar paquetes VTP para añadir, cambiar o borrar la información sobre las VLANs. Existen herramientas disponibles gratuitamente para realizar esas operaciones. Debido a eso se recomienda establecer un password para el dominio VTP y usarlo en conjunto con la función hash MD5 para proveer autenticación a los paquetes VTP. y tan importante es para los enlaces truncales de la vlan.

- Se lo emplea para distribuir configuraciones de VLAN a través de múltiples dispositivos.
- VTP se emplea únicamente en puertos trunk.
- VTP puede causar muchos inconvenientes.

- VTP emplea autenticación considere usar MD5.
- Si un atacante logra que su puerto se convierta en trunk, puede enviar mensajes VTP como si fuera un servidor VTP sin VLANs configuradas. Cuando los demas switches reciban el mensaje eliminarán todas sus VLANs.

2.3. Ataques basados en STP

Spanning Tree Protocol (SmmTPr) es un protocolo de red de nivel 2 de la capa OSI, (nivel de enlace de datos). Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC. Hay 2 versiones del STP: la original (DEC STP) y la estandarizada por el IEEE (IEEE 802.1D), que no son compatibles entre sí. En la actualidad, se recomienda utilizar la versión estandarizada por el IEEE.

Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de bucles. STP es transparente a las estaciones de usuario.

Los bucles infinitos ocurren cuando hay rutas alternativas hacia una misma máquina o segmento de red de destino. Estas rutas alternativas son necesarias para proporcionar redundancia, ofreciendo una mayor fiabilidad. Si existen varios enlaces, en el caso que uno falle, otro enlace puede seguir soportando el tráfico de la red. Los problemas aparecen cuando utilizamos dispositivos de interconexión de nivel de enlace, como un puente de red o un conmutador de paquetes.

Cuando hay bucles en la topología de red, los dispositivos de interconexión de nivel de enlace reenvían indefinidamente las tramas Broadcast y multicast, al no existir ningún campo TTL (Time To Live, Tiempo de Vida) en la Capa 2, tal y como ocurre en la Capa 3. Se consume entonces una gran cantidad de ancho de banda, y en muchos caso la red queda inutilizada. Un router, por el contrario, sí podría evitar este tipo de reenvíos indefinidos. La solución consiste en permitir la existencia de enlaces físicos redundantes, pero creando una topología lógica libre de bucles. STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (esto previene los bucles) pero mantiene los caminos redundantes como reserva, para activarlos en caso de que el camino inicial falle.

Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces de reserva. Si el protocolo falla, es posible que ambas conexiones estén activas simultáneamente, lo que podrían dar lugar a un bucle de tráfico infinito en la LAN.

Existen múltiples variantes del Spaning Tree Protocol, debido principalmente al tiempo que tarda el algoritmo utilizado en converger. Una de estas variantes es el Rapid Spanning Tree Protocol

El árbol de expansión (Spanning tree) permanece vigente hasta que ocurre un cambio en

la topología, situación que el protocolo es capaz de detectar de forma automática. El máximo tiempo de duración del árbol de expansión es de cinco minutos. Cuando ocurre uno de estos cambios, el puente raíz actual redefine la topología del árbol de expansión o se elige un nuevo puente raíz.

2.3.1. Funcionamiento

Este algoritmo cambia una red física con forma de malla, en la que existen bucles, por una red lógica en árbol en la que no existe ningún bucle. Los puentes se comunican mediante mensajes de configuración llamados Bridge Protocol Data Units (B.P.D.U).

El protocolo establece identificadores por puente y elige el que tiene la prioridad más alta (el número más bajo de prioridad numérica), como el puente raíz. Este puente raíz establecerá el camino de menor coste para todas las redes; cada puerto tiene un parámetro configurable: el Span path cost. Después, entre todos los puentes que conectan un segmento de red, se elige un puente designado, el de menor coste (en el caso que haya mismo coste en dos puentes, se elige el que tenga el menor identificador "direccion MAC"), para transmitir las tramas hacia la raíz. En este puente designado, el puerto que conecta con el segmento, es el puerto designado y el que ofrece un camino de menor coste hacia la raíz, el puerto raíz. Todos los demás puertos y caminos son bloqueados, esto es en un estado ya estacionario de funcionamiento.

2.3.2. Elección Del Puente Raíz

La primera decisión que toman todos los switches de la red es identificar el puente raíz ya que esto afectará al flujo de tráfico. Cuando un switch se enciende, supone que es el switch raíz y envía las BPDU que contienen la dirección MAC de sí mismo tanto en el BID raíz como emisor. Cada switch reemplaza los BID de raíz más alta por BID de raíz más baja en las BPDU que se envían. Todos los switches reciben las BPDU y determinan que el switch que cuyo valor de BID raíz es el más bajo será el puente raíz. El administrador de red puede establecer la prioridad de switch en un valor más pequeño que el del valor por defecto (32768), lo que hace que el BID sea más pequeño. Esto sólo se debe implementar cuando se tiene un conocimiento profundo del flujo de tráfico en la red.

2.3.3. Elección De Los Puertos Raíz

Una vez elegido el puente raíz hay que calcular el puerto raíz para los otros puentes que no son raíz. Para cada puente se calcula de igual manera, cual de los puertos del puente tiene menor coste al puente raíz, ese será el puerto raíz de ese puente.

2.3.4. Elección De Los Puertos Designados

Una vez elegido el puente raíz y los puertos raíz de los otros puentes pasamos a calcular los puertos designados de cada LAN, que será el que le lleva al menor coste al puente raíz. Si hubiese empate se elige por el ID más bajo.

2.3.5. Puertos Bloqueados

Aquellos puertos que no sean elegidos como raíz ni como designados deben bloquearse.

2.3.6. Mantenimiento del Spanning Tree

El cambio en la topología puede ocurrir de dos formas:

- El puerto se desactiva o se bloquea
- El puerto pasa de estar bloqueado o desactivado a activado

Cuando se detecta un cambio el switch notifica al puente raíz dicho cambio y entonces el puente raíz envía por broadcast dicha cambio. Para ello, se introduce una BPDU especial denominada notificación de cambio en la topología (TCN). Cuando un switch necesita avisar acerca de un cambio en la topología, comienza a enviar TCN en su puerto raíz. La TCN es una BPDU muy simple que no contiene información y se envía durante el intervalo de tiempo de saludo. El switch que recibe la TCN se denomina puente designado y realiza el acuse de recibo mediante el envío inmediato de una BPDU normal con el bit de acuse de recibo de cambio en la topología (TCA). Este intercambio continúa hasta que el puente raíz responde.

2.3.7. Estado De Los Puertos

Los estado en los que puede estar un puerto son los siguientes:

- Bloqueo: En este estado se pueden recibir BPDU's pero no las enviará. Las tramas de datos se descartan y no se actualizan las tablas de direcciones MAC (mac-address-table).
- Escucha: A este estado se llega desde Bloqueo. En este estado, los switches determinan si existe alguna otra ruta hacia el puente raíz. En el caso que la nueva ruta tenga un coste mayor, se vuelve al estado de Bloqueo. Las tramas de datos se descartan y no se actualizan las tablas ARP. Se procesan las BPDU.
- Aprendizaje: A este estado se llega desde Escucha. Las tramas de datos se descartan pero ya se actualizan las tablas de direcciones MAC (aquí es donde se aprenden por primera vez). Se procesan las BPDU.
- Envío: A este estado se llega desde Aprendizaje. Las tramas de datos se envían y se actualizan las tablas de direcciones MAC (mac-address-table). Se procesan las BPDU.
- Desactivado: A este estado se llega desde cualquier otro. Se produce cuando un administrador deshabilita el puerto o éste falla. No se procesan las BPDU.

2.3.8. Ataques Basados En STP

- El atacante envía mensajes BPDU forzando recálculos STP.

- El atacante envía mensajes BPDU para convertirse en root.
- El atacante se convierte en root con lo cual puede ver tramas que no debería (esto permite ataques MiM, DoS, etc)
- Hace falta que el atacante este conectado a dos switches simultáneamente.

2.3.9. ¿Como Trabaja?.

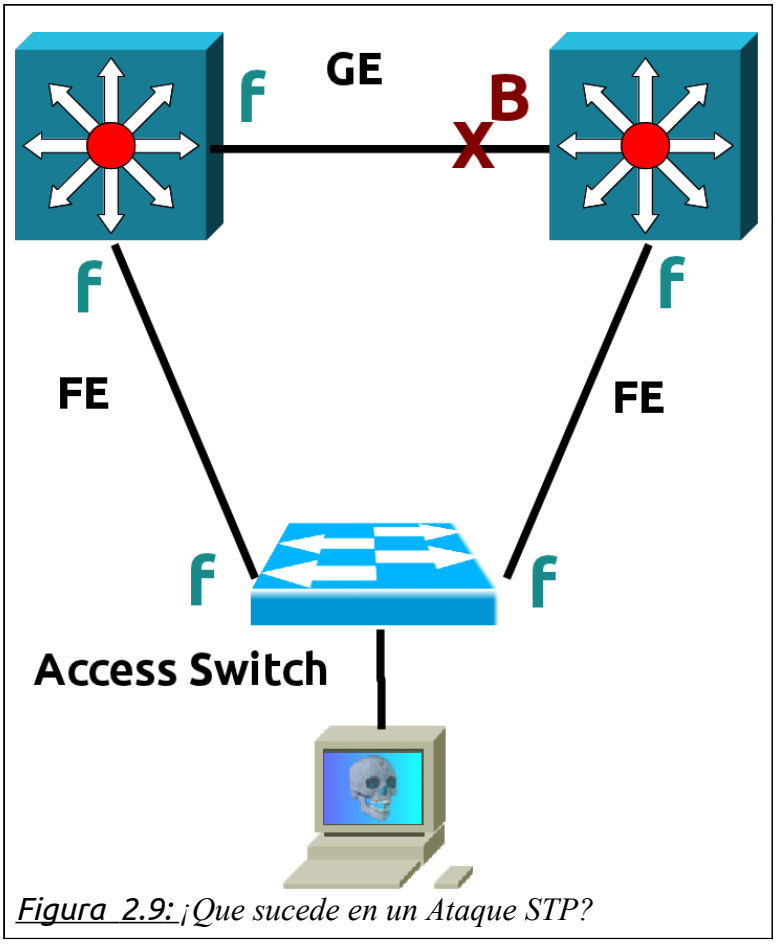


Figura 2.9: ¡Que sucede en un Ataque STP?

- El atacante envía mensajes BPDU anunciándose como bridge con prioridad 0.
- El atacante se vuelve root.
- El backbone pasa de ser GE a ser FE.
- Si se lo combina con MAC flooding este ataque puede permitir capturar más tramas.

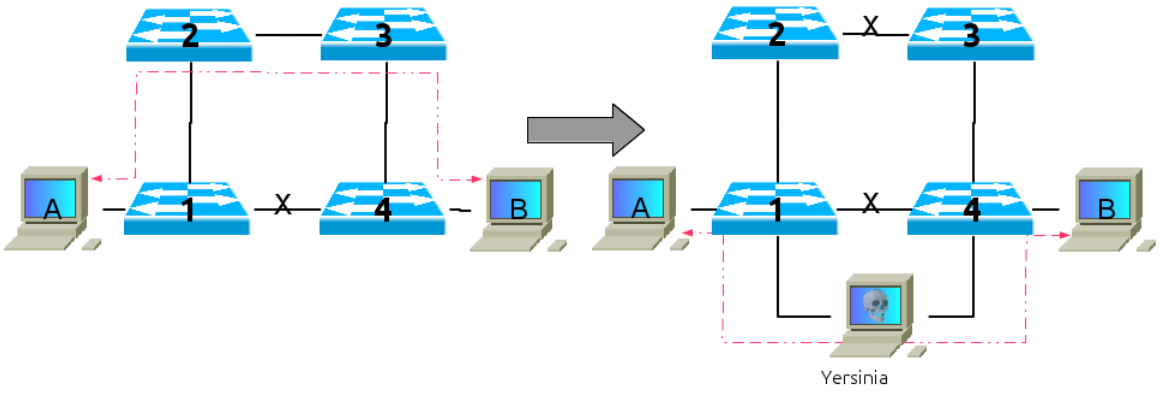


figura 2.10: Simulando un ataque a un Switch de Alojamiento Dual

3. CONTRAMEDIDAS

3.1. Ataques MAC Y ARP

3.1.1. Storm Control.

Una tormenta de paquetes ocurre cuando se reciben en un puerto gran número de paquetes broadcast, unicast o multicast. Reenviar esos paquetes puede causar una reducción de la performance de la red e incluso la interrupción del servicio. Storm Control usa umbrales para bloquear y restaurar el reenvío de paquetes broadcast, unicast o multicast. Usa un método basado en ancho de banda. Los umbrales se expresan como un procentaje del total de ancho de banda que puede ser empleado para cada tipo de tráfico.

3.1.1.1. CONFIGURACIÓN STORM-CONTROL

Deseamos configurar el puerto 15 del switch para que si el tráfico broadcast supere el 45% del ancho de banda disponible envíe una alerta.

Las opciones completas son:

Table 3.1: Configuración Storm Control

	Comando	Propósito
Paso 1	*Router(config)# **interface** {{type[1] slot/port} | {**port-channel** number}}*	Seleciona una interfaz para configurar.
Paso 2	*Router(config-if)# **storm-control broadcast level** level[.level]*	Habilita el tráfico broadcast storm-control en la interfaz, configura el nivel de tráfico storm-control y aplica el nivel de tráfico storm-control a todos los modos de tráfico storm-control habilitados en el puerto.
	*Router(config-if)# **no storm-control broadcast level***	Deshabilita el tráfico broadcast storm-control en el puerto.
Paso 3	*Router(config-if)# **storm-control multicast level** level[.level]* ***Note** The **storm-control multicast** command is supported only on Gigabit Ethernet interfaces.*	Habilita el tráfico multicast storm-control en la interfaz, configura el nivel de tráfico storm-control y aplica el nivel de tráfico storm-control a todos los modos de tráfico storm-control habilitados en el puerto.
	*Router(config-if)# **no storm-control multicast level***	Deshabilita el tráfico multicast storm-control en el puerto.
Paso 4	*Router(config-if)# **storm-control unicast level** level[.level]* ***Note** The **storm-control unicast** command is supported only on Gigabit Ethernet interfaces.*	Habilita el tráfico unicast storm-control en la interfaz, configura el nivel de tráfico storm-control, y aplica el nivel de tráfico a todos los modos de tráfico storm-control habilitados en la interfaz.
	*Router(config-if)# **no storm-control unicast level***	Desabilita el tráfico unicast storm-control en la interfaz.
Paso 5	*Router(config-if)# **end***	Sale del modo de configuración.
Paso 6	*Router# **show running-config** interface*	Verifica la configuración.

3.1.2. Puertos Protegidos.

Ciertas aplicaciones requieren que nos se reenvíe tráfico entre puertos en un mismo switch de manera que un equipo no ve el tráfico generado por otro (inclusive tráfico broadcast y
multicast).

- No se puede reenviar tráfico entre puertos protegidos a nivel de capa 2.
- El tráfico entre puertos protegidos debe ser reenviado a través de un dispositivo de capa 3.
- El reenvio de tráfico entre puertos protegidos y no protegidos se realiza de manera normal.

3.1.2.1. CONFIGURACIÓN PARA UN PUERTO PROTEGIDO.

Table 3.2: Para configurar un puerto como protegido.

	Comando	Propósito
Paso 1	***Configure terminal***	Entra al modo de configuración global.
Paso 2	***Interface*** *interface id*	Especifica el puerto a ser configurada, y entra al modo de configuración de el puerto.
Paso 3	***Switchport protected***	Configura el puerto para ser un puerto protegido.
Paso 4	***end***	Retorna al modo EXEC privilegiado.
Paso 5	***Show interfaces*** *interface-id switchport*	Verifica tus entradas.
Paso 6	***Copy running-config start-up config***	(Opcional) Guarda tus entradas y el archivo de configuración.

3.1.3. Port Security.

Conjunto de medidas de seguridad a nivel de puertos disponibles en la mayoría de los switchs de gama media y alta. La funciones provistas dependen de la marca, el modelo y la versión de firmware del switch en cuestión. Permite entre otras cosas:

- Restringir el acceso a los puertos según la MAC.
- Restringir el numero de MACs por puerto.
- Reaccionar de diferentes maneras a violaciones de las restricciones anteriores.
- Establecer la duración de las asociaciones MAC-Puerto.

3.1.3.1. **CONFIGURACION PORT-SECURITY**

Deseamos configurar el puerto 15 del switch para que no acepte más de dos direcciones MAC.

- No se puede activar port security en puertos dynamic access o trunk.
- Port Security está desactivado por default.
- Por default port security sólo almacena una sola MAC por puerto.

Además podemos especificar qué hacer si ese número de direcciones MAC es superado (por default deshabilitar el puerto):

- Que deje de aprender
- Que envíe una alerta administrativa
- Que deshabilite el puerto

	Comando	Propósito
Paso 1	*Switch(config)#* ***interface*** *interface_id*	Entra en el modo de configuración de el puerto para configurar, por ejemplo gigabitethernet 3/1.
Paso 2	*Switch(config-if)#* ***switchport mode access***	Coloca el modo de el puerto en access; un puerto en el modo por defecto (dynamic desirable) no puede ser configurada como puerto seguro
Paso 3	*Switch(config-if)#* ***switchport port-security***	Habilita Port-security en la interfaz.
Paso 4	*Switch(config-if)#* ***switchport port-security maximum*** *value*	(Opcional) Coloca el máximo número de direcciones MAC seguras para el puerto. El rango es de 1 a 1024: por defecto está en 1.

Tabla 3.3: Configuración Port-security

3.2. Seguridad Capa 2: VLAN Privadas.

Para prevenir este tipo de ataques debemos hacer lo siguiente:

- Deshabilitar auto trunking para todos los puertos:
- Deshabilitar VTP:
- Si es realmente necesario, usar la versión 2.
- Siempre utilizar una VLAN dedicada para los puertos trunk.
- Deshabilitar los puertos no utilizados y colocarlos en una VLAN no utilizada.
- No utilizar la VLAN 1 para nada.
- Colocar todos los puertos de los usuarios como non-trunking (Deshabilitar DTP).

3.3. Ataques STP

- No deshabilitar STP (introducir un loop puede convertirse en una forma de ataque).
- Habilitar BPDU Guard.
- Habilitar Root Guard.

4. PRACTICAS

4.1. Practica 1 (Mac Flooding Attack)

4.1.1. ESCENARIO.

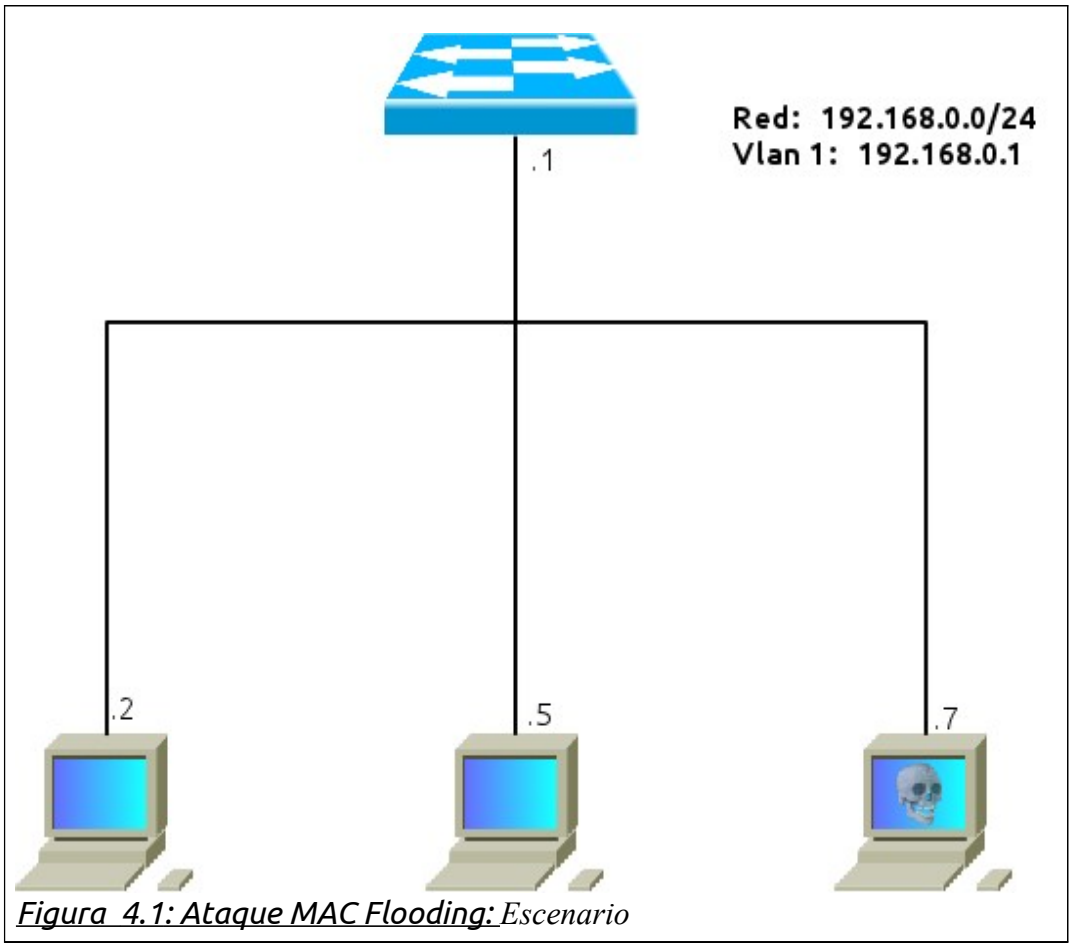


Figura 4.1: Ataque MAC Flooding: Escenario

4.1.1.1. HARWARE

- 3 terminales con sistema Operativo linux y distribuci{on Fedora o Ubuntu.
- 1 Switch Catalyst Cisco 3560.

4.1.1.2. SOFTWARE

- Yakuake.
- Cutecom.
- Dsniff.

Nota. Cosulte los anexos: Configuraci{on de IP estática para la configuracin de la IP en los equipos de linux

4.1.1.3. YAKUAKE

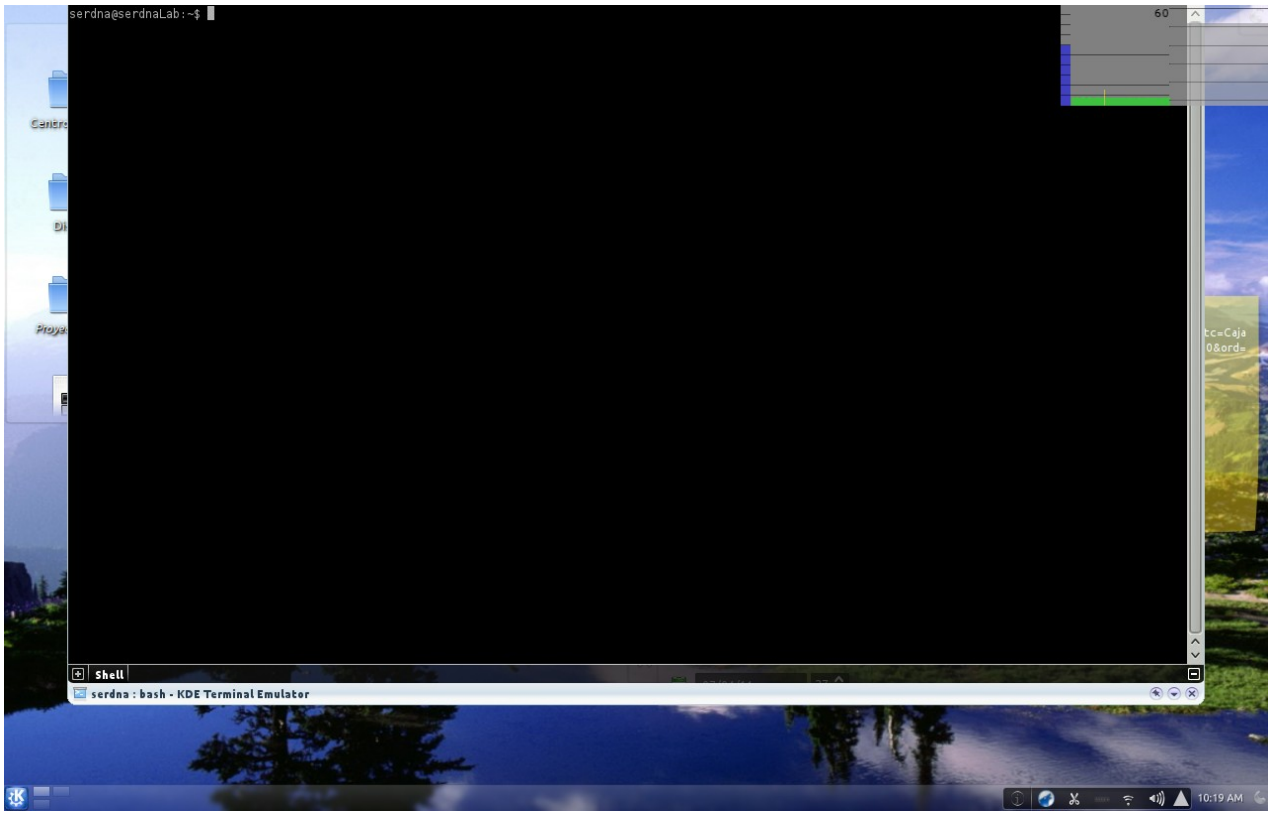


Figura 4.2: Yakuake

Yakuake esta inspirado en la terminal del Juego Quake, cuando presionas en el teclado (por defecto la tecla F12 que puede ser modificada) una ventana se desliza hacia abajo desde la parte superior de la pantalla, y si se vuelve a oprimir la tecla esta retorna, lo que nos da una mayor comodidad y rapidez a la konsola de comandos de linux.

4.1.1.3.1.1. Instalación de yakuake

Para su instalación la podemos realizar de dos formas una desde el administrador de paquetes de linux escribimos yakuake u otra desde la consola de comandos (figura 4.3).

Accedemos como root (consultar con el administrador del laboratorio para acceder como root) y desde la consola de comandos digitamos el comando.

Desde fedora:
[labdisca04@labdisca04:~$] su -

[root@labdisca04 ~]#

*[root@labdisca04 ~]# **yum install** yakuake*

Desde Ubuntu: (Figura 4.3)

labdisca04@labdiscaxx:/home/labdisca# su

Password:

root@labdisca04:/home/labdisca#

*root@labdiscaxx /home/labdiscaxx #**apt-get install** yakuake*

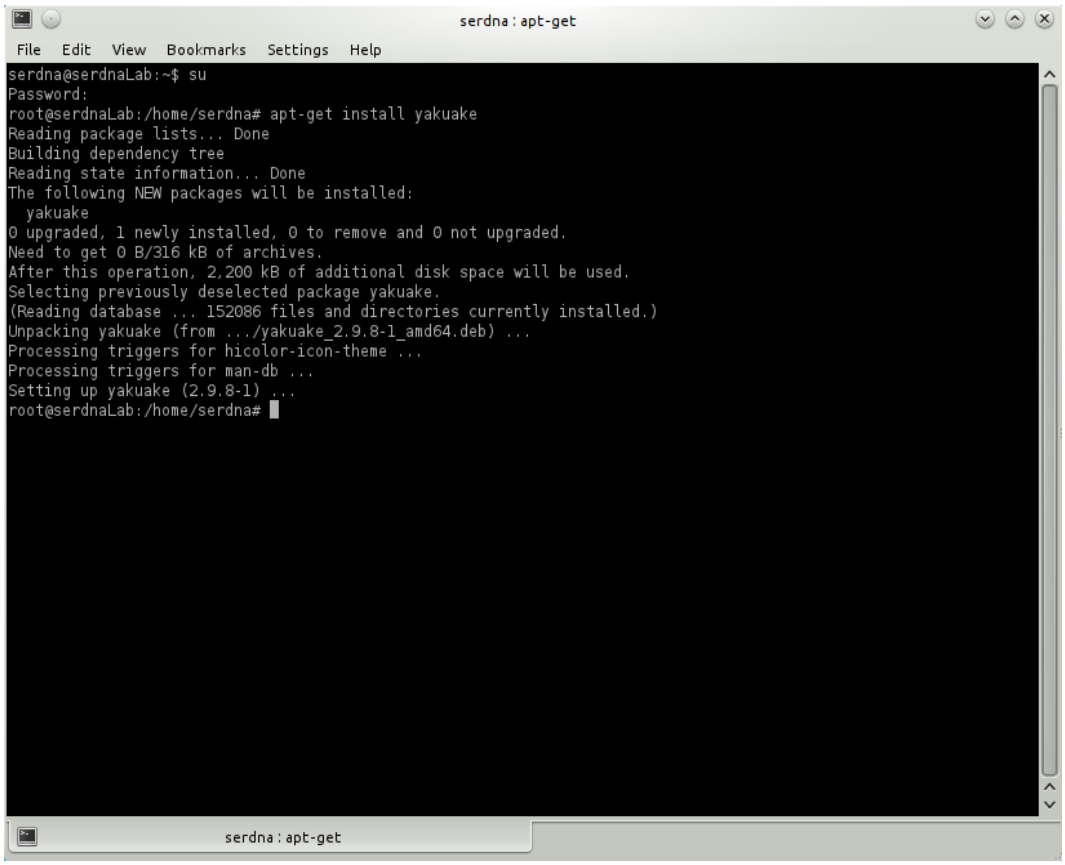


Figura 4.3: Paso 1:Yakuake: Instalación

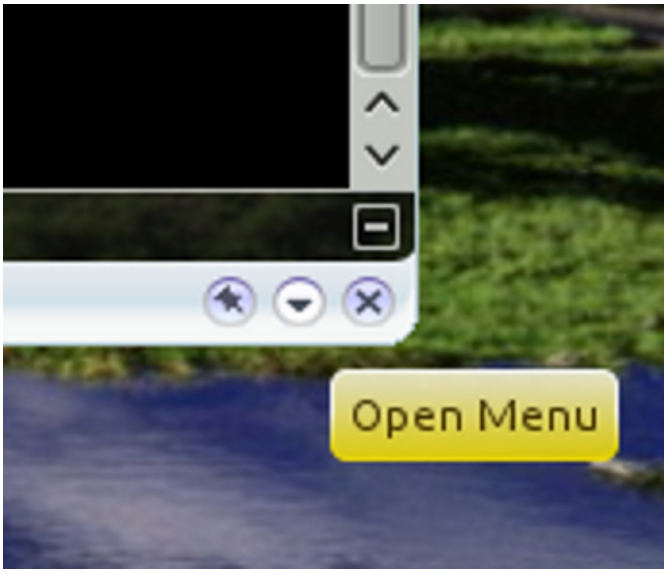
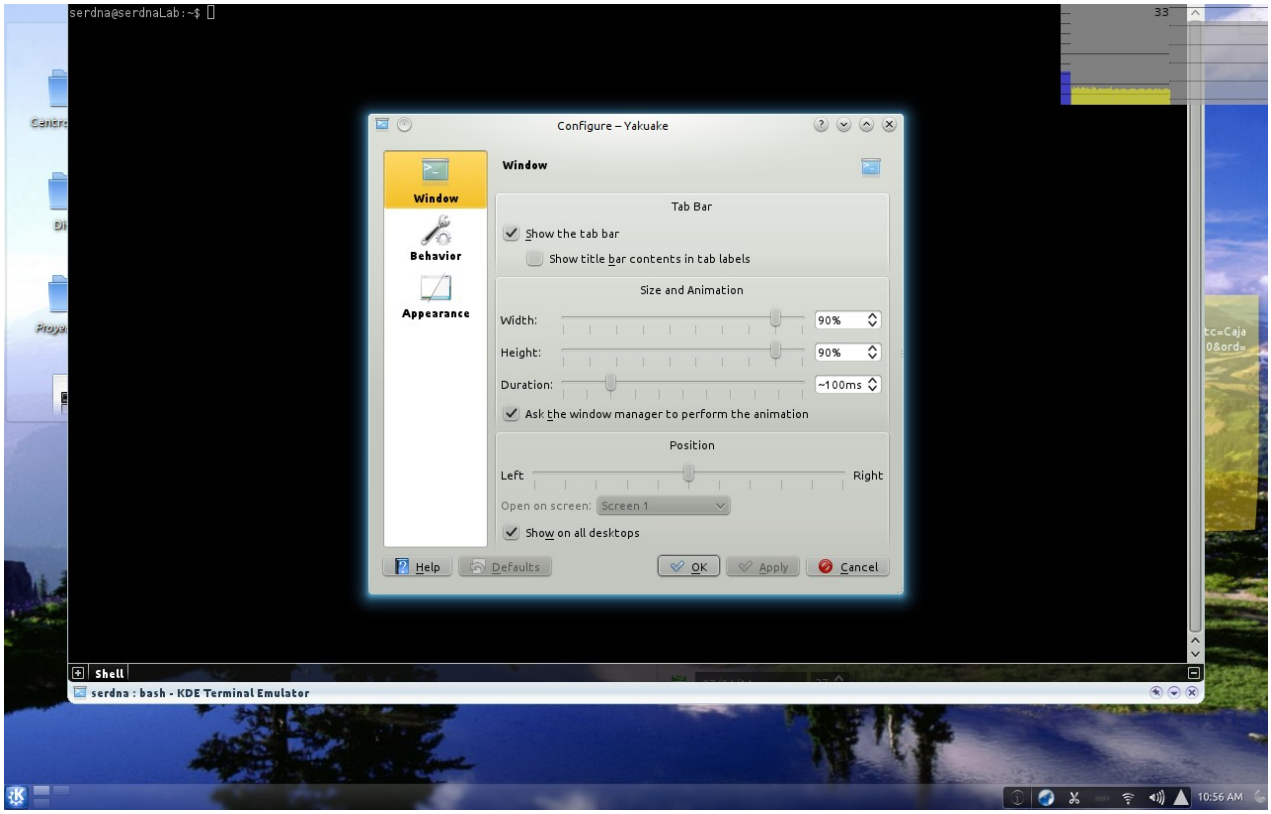


Figura 4.4: Paso 3: Yakuake Accediendo al menú

Para ejecutar yakuake presionamos la tecla configurada (en su defecto F12) y nuestra ventana se desliza hacia abajo desde la parte superior de la pantalla (figura

4.2).Configuración de Yakuake
Acedemos al menú (figura 4.4) desde la parte inferior derecha de la consola.



IFigura 4.5: Paso 4: Yakuake: Configuración de yakuake

Para acceder a la configuracion de yakuake selecionamos desde la ventana desplegable "configuración de yakuake" se nos muestra una nueva ventana (figura 4.5) y modificamos los valores a nuestras necesidades. Tal como la configuración de la ventana, comportamiento y apariencia.

4.1.1.3.2. Cutecom

Es un terminal serial gráfico, como minicom[13] Está dirigido a desarrolladores de hardware u otras personas que necesitan una terminal para comunicarse con sus dispositivos. Esta característica es lineo-orientada a terminal en vez de ser orientada a carácter, con soporte xmodem, ymodem y zmodem.

4.1.1.3.2.1. Instalación Cutecom.

- Accedemos como Root consultar " capítulo **4.1.1.2.1.1.** Instalación de yakuake"
- Si estamos en fedora digitamos el comando:
  yum install *cutecom.*

  si estamos en Ubuntu

a ***pt-get install*** *cutecom.*

13 *Es un programa de comunicación, que de alguna manera reensambla el programa compartido TELIX pero con un código fuente ue se puede ejecutar en la mayoría de sistemas UNIX. (TELIX: Programa de Telecomunicación originalmente escrito en DOS por Colin Sampaleanu y lanzado en 1986).*

- Si nuestra instalación fue correcta no nos debe mostrar errores en la instalación.
- Como root ejecutamos cutecom desde yakuake.

  [root@labdisca04 ~]# cutecom (*Figura 4.6*)

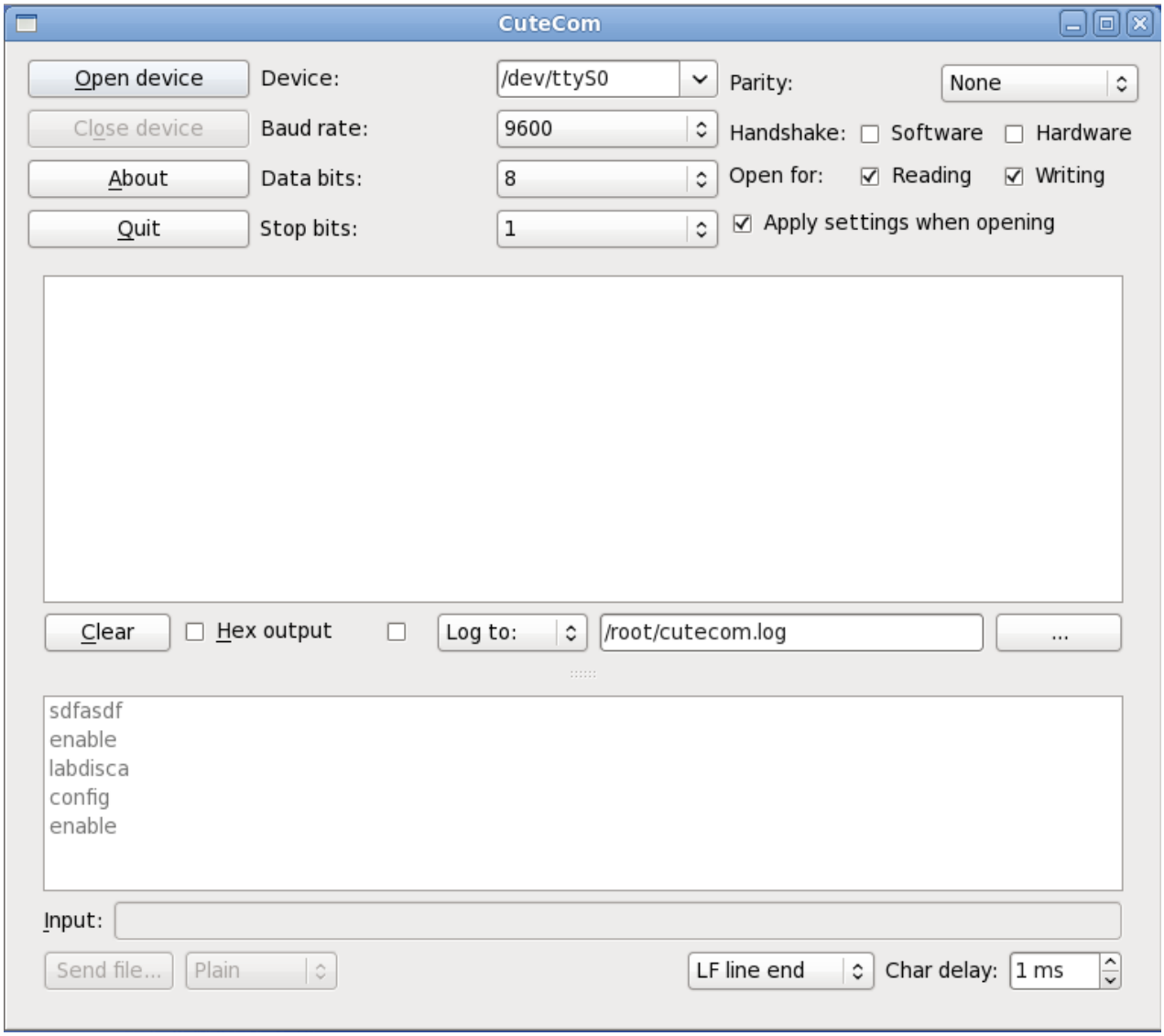


Figura 4.6: Paso 4: Cutecom: Iniciando

4.1.1.3.2.2. Cofiguración de cutecom

Como se muestra en la (figura 4.6).

- **Device:** Para reconocer cual es nuestro dipositivo activo digitamos los siguientes comandos:
  [root@labdiscaxx ~]# dmesg | grep tty
  console [tty0] enabled
  serial8250: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
  00:08: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
  En nuestro caso nuestro dispositivo activo es ttyS0.

Device: /dev/ttyS0

- **Baudrate:** 9600
- **Bits de Datos:** 8
- **Bits de parada:** 1
- **Paridad:** ningura (none)

4.1.1.3.2.3. Ejecutando cutecom (Figura 4.7)

- Colocamos el modo de entrada: CR, LF line end.

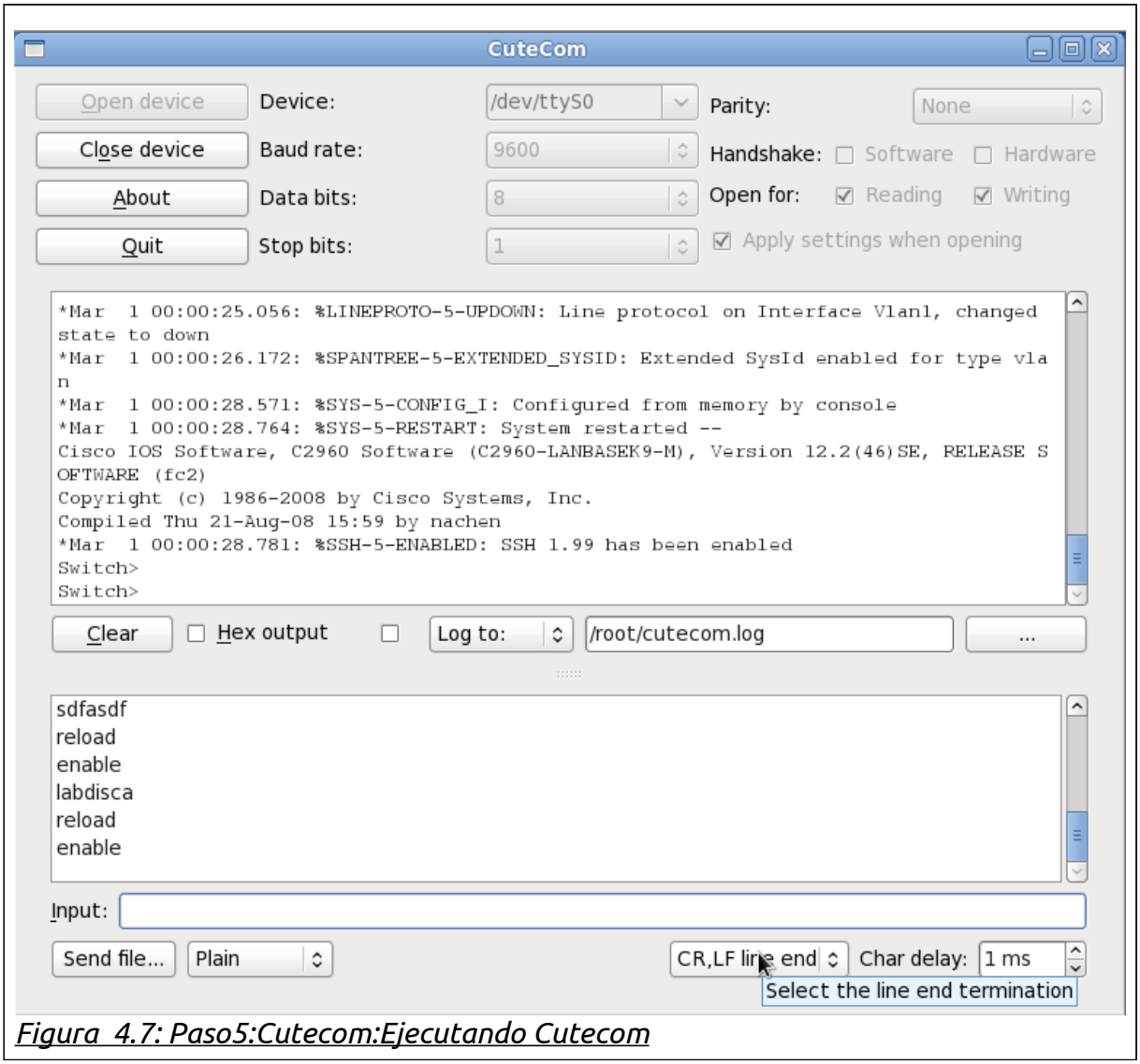


Figura 4.7: Paso5:Cutecom:Ejecutando Cutecom

Paso 1: Ejecutamos nuestro terminal en "Open device"
Paso 2: En la casilla input tipeamos enable para poner nuestro Switch en modo EXEC.()
Switch> enable

Paso 3: Configuramos el Switch

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname ALS1 (Nombre del switch ALS1)

ALS1(config)#interface vlan 1 (entramos a configurar Vlan 1)

ALS1(config-if)#ip address 192.168.0.1 255.255.255.0 (Le asignamos una ip y su respectiva máscara)

ALS1(config-if)#no shutdown (Activamos Vlan 1)

%LINK-5-CHANGED: Interface Vlan1, changed state to up

ALS1(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

ALS1(config-if)#end Salimos del modo de configuración.

%SYS-5-CONFIG_I: Configured from console by console

ALS1#

4.1.1.3.3. Dsniff

Es una colección de herramientas para auditar la red y pruebas de penetración. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy monitorean la red de forma pasiva para recopilar datos de interes. (contraseñas, correos electrónicos, archivos, etc). arpspoof, dnsspoof, y macof facilitan facilitan la intercepción del tráfico de red normalmente inaccecible para un atacante (Por ejemplo. Debido a los switches de capa 2). sshmitm y webmitm implementan ataques activos man-in-the-middle contra redirecci{on de sessiones SSH[14] y HTTPS[15] por explotación de enlaces débiles en PKI ad-hoc[16].

4.1.1.3.3.1. Para Monitorear La Red De Forma Pasiva.

Dsniff.captura de contraseñas para FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft, SMB, Oracle SQL*Net, Sybase y Microsoft SQL.
Filesnarf. Vertederos de todos los archivos enviados vía NFS.
Mailsnarf. Vertederos de e-mail en formato leible de SMTP y POP.
Msgsnarf. Vertederos de emensajes instantáneos
Urlsnarf. Captura url's en http.
Webspy. Espejos de paginas web buscadas por un usuario en tiempo real

4.1.1.3.3.2. Intercepción del tráfico de red.

Arpspoof. Envenena un objetivo cache de ARP.
Dnsspoof. Envenena un objetivo de busquedas DNS

---

14 ***SSH: Secure Shell:*** *Interprete de ordenes segura*
15 ***Hyper Text Transfer Protocol Secure*** *(en español: Protocolo seguro de transferencia de hipertexto)*
16 ***PKI Ad-hoc:*** *Provee un mecanismo para manejar criptografia de claves. En redes Ad-hoc*

Macof. Inunda switches con MAC's hasta hacerlos fallar y convertirlos en repetidores.

4.1.1.3.3.3. Implementan ataques activos man-in-the-middle.

Sshmitm. Realiza ssh MITM.
Webmitm. Realiza un ssl[17] MITM.

4.1.1.3.3.4. Instalacion Dsniff

Paso 4: Desde root en fedora digitamos el comando:

*[root@labdisca04 ~]# **yum install** dsniff*

---

*[root@labdisca04 ~]# **yum install** dsniff*
Complementos cargados:presto, refresh-packagekit
Bloqueo existente en /var/run/yum.pid: otra copia se encuentra en ejecución como pid 2626.
Otra aplicación tiene retenido el bloqueo de Yum; esperándolo para salir...
La otra aplicación es: PackageKit
Memoria : 46 M RSS (60 MB VSZ)
Iniciado: Wed Jan 12 13:56:34 2011 - 00:03 atrás
Estado : Ejecutando, pid: 2626
Otra aplicación tiene retenido el bloqueo de Yum; esperándolo para salir...
La otra aplicación es: PackageKit
Memoria : 84 M RSS (98 MB VSZ)
Iniciado: Wed Jan 12 13:56:34 2011 - 00:05 atrás
Estado : Durmiendo, pid: 2626
Otra aplicación tiene retenido el bloqueo de Yum; esperándolo para salir...
La otra aplicación es: PackageKit
Memoria : 84 M RSS (98 MB VSZ)
Iniciado: Wed Jan 12 13:56:34 2011 - 00:07 atrás
Estado : Durmiendo, pid: 2626
Otra aplicación tiene retenido el bloqueo de Yum; esperándolo para salir...
La otra aplicación es: PackageKit
Memoria : 84 M RSS (98 MB VSZ)
Iniciado: Wed Jan 12 13:56:34 2011 - 00:09 atrás
Estado : Durmiendo, pid: 2626
Configurando el proceso de instalación
Resolviendo dependencias
--> Ejecutando prueba de transacción

17 ***SSL: Secure Sockets Layer.*** *Protocolo de capa de conexión segura*

---> Paquete dsniff.i686 0:2.4-0.9.b1.fc13 definido para ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

==
Paquete Arquitectura Versión Repositorio Tamaño
==
Instalando:
dsniff i686 2.4-0.9.b1.fc13 fedora 101 k

Resumen de la transacción
==
Install 1 Package(s)
Tamaño total de la descarga: 101 k
Tamaño instalado: 269 k
Está de acuerdo [s/N]:s
Descargando paquetes:
Setting up and reading Presto delta metadata
Processing delta metadata
Package(s) data still to download: 101 k
dsniff-2.4-0.9.b1.fc13.i686.rpm | 101 kB 00:00
Ejecutando el rpm_check_debug
Ejecutando prueba de transacción
La prueba de transacción ha sido exitosa
Ejecutando transacción
Instalando : dsniff-2.4-0.9.b1.fc13.i686 1/1

Instalado:
dsniff.i686 0:2.4-0.9.b1.fc13

¡Listo!

Desde Ubuntu

root@labdisca:/home/labdisca# **apt-get install** dsniff

4.1.1.3.3.5. Ejecutando dsniff.

Abrimos yakuake (pulsamos F12 por defecto) y como root digitamos el comando:

root@labdisca:/home/labdisca# **cutecom**
Desde cutecom con modo de entrada "CR, LF line end" escribimos:

Paso 5: Desde el switch con cutecom observamos nuestra tabla mac addres-table count ue nos muestra la cantidad de macs asignadas.

show MAC address-table count

Este comando nos muetra en numero de direcciones MAC utilizadas y el total de direcciones MAC disponibles:

En nuestro caso (figura 4.8)

- Cantidad Direcciones estáticas usadas: 0
- Cantidad de direcciones dinámicas usadas: 0.
- Cantidad de direcciones MAC disponibles: 5567.

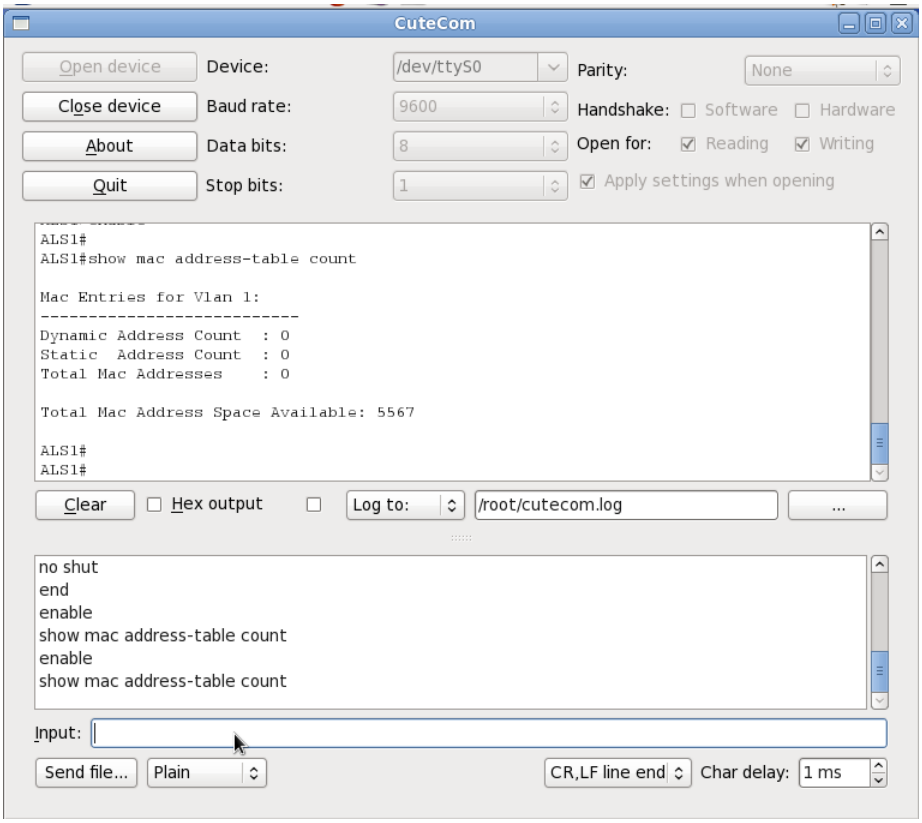


Figura 4.8: Paso 5: MAC flooding: Tabla de contéo MAC

Para el ataque por inundamiento de MAC's usaremos la herramienta macof de dsniff

¡Importante!. Este ataque puede colapsar una red por eso debemos asegurarnos que la interfaz que vamos a usar sea una red creada por nosotros para ello ejecutamos el comando "ifconfig" y nos aseguramos de usar la interfaz correcta. En mi caso use la interfaz eth3.

Paso6: Como root en nuestra consola de comandos yakuake digitamos el comando:

[root@labdisca04 ~]# macof -i eth3

Aqui comienza nuestro ataque..

53:1e:43:4c:35:c8 2f:b2:30:7e:ee:c 0.0.0.0.30486 > 0.0.0.0.49942: S 961023746:961023746(0) win 512

2a:4f:5b:10:25:36 65:81:6c:35:7a:6c 0.0.0.0.21499 > 0.0.0.0.3740: S 1055267698:1055267698(0) win 512

b9:5e:3a:6f:e2:9b a7:92:e7:49:a6:49 0.0.0.0.35379 > 0.0.0.0.64005: S 1362531159:1362531159(0) win 512

da:24:9:17:23:cf f2:d8:e5:59:42:ec 0.0.0.0.63081 > 0.0.0.0.21289: S 188090032:188090032(0) win 512

a7:f0:4:22:6c:71 56:0:84:74:7d:c9 0.0.0.0.55353 > 0.0.0.0.45537: S 1922743052:1922743052(0) win 512

be:1c:fc:d:9a:7b b0:e1:c4:6c:49:7 0.0.0.0.32637 > 0.0.0.0.53107: S 401293249:401293249(0) win 512

7e:2e:99:b:90:93 23:7c:c:37:ef:6c 0.0.0.0.48063 > 0.0.0.0.30270: S 830091504:830091504(0) win 512

c6:f2:2b:42:17:75 30:ee:e1:50:cc:29 0.0.0.0.18647 > 0.0.0.0.5838: S 1146686082:1146686082(0) win 512

a3:af:bd:19:95:79 ad:c5:6b:2c:d5:97 0.0.0.0.30076 > 0.0.0.0.32859: S 1165148507:1165148507(0) win 512

3f:d8:27:c:e5:40 c:f5:ac:6b:96:97 0.0.0.0.42711 > 0.0.0.0.59796: S 375668839:375668839(0) win 512

44:21:f6:15:bd:8b f4:da:65:23:4d:76 0.0.0.0.37701 > 0.0.0.0.32353: S 1362788995:1362788995(0) win 512

d:c3:d2:31:1e:9d e3:b6:d2:24:f9:e6 0.0.0.0.7764 > 0.0.0.0.10864: S 1101044559:1101044559(0) win 512

98:a4:0:53:56:c1 c2:51:45:14:52:d8 0.0.0.0.14560 > 0.0.0.0.32709: S 729141755:729141755(0) win 512

b8:9:50:7f:ab:34 eb:3d:7d:5d:62:7 0.0.0.0.50256 > 0.0.0.0.48702: S 1408858971:1408858971(0) win 512

79:17:e6:8:34:44 ed:7:3f:2d:15:fc 0.0.0.0.55466 > 0.0.0.0.51585: S 889315214:889315214(0) win 512

99:c9:a:25:29:8c c4:6a:2d:c:ab:54 0.0.0.0.26759 > 0.0.0.0.7516: S 1284735760:1284735760(0) win 512

e1:f2:25:3a:ab:d8 a1:29:2:71:6f:48 0.0.0.0.39266 > 0.0.0.0.9311: S 1336849452:1336849452(0) win 512

80:9a:ec:21:3a:24 c5:4e:26:5e:99:f1 0.0.0.0.56249 > 0.0.0.0.63737: S 604143001:604143001(0) win 512

1e:ed:76:41:3f:90 8a:d1:e9:2a:86:a5 0.0.0.0.62820 > 0.0.0.0.52593: S 651351929:651351929(0) win 512

56:fd:13:36:53:2b 6f:9a:45:3:e:4e 0.0.0.0.37802 > 0.0.0.0.3365: S 1367658653:1367658653(0) win 512

85:a0:56:55:8e:de 1f:d3:9f:68:c8:22 0.0.0.0.31458 > 0.0.0.0.44002: S 1912562442:1912562442(0) win 512

c3:c8:69:53:9e:83 0:ca:bd:62:a1:18 0.0.0.0.63888 > 0.0.0.0.40586: S 1805185922:1805185922(0) win 512

48:40:4b:23:85:12 76:2b:b9:77:48:1 0.0.0.0.65290 > 0.0.0.0.29757: S 1834071749:1834071749(0) win 512

98:72:2a:19:f2:99 56:22:66:5d:82:47 0.0.0.0.9106 > 0.0.0.0.47004: S 1350937409:1350937409(0) win 512

97:ce:83:5:f3:97 d:66:2d:16:d9:0 0.0.0.0.4737 > 0.0.0.0.43556: S 53559480:53559480(0) win 512

10:f9:f0:28:7c:a7 7f:a9:a2:5a:30:45 0.0.0.0.23586 > 0.0.0.0.42960: S 746925166:746925166(0) win 512

8c:f9:71:4f:b5:e4 32:59:f9:40:ba:48 0.0.0.0.39070 > 0.0.0.0.53193: S 586279825:586279825(0) win 512

7d:ad:e8:1a:9d:e2 9:6b:50:41:a0:44 0.0.0.0.27135 > 0.0.0.0.30200: S 1975783759:1975783759(0) win 512

8a:d0:9:17:15:29 5a:e3:b:72:b5:eb 0.0.0.0.20587 > 0.0.0.0.51815: S 613843302:613843302(0) win 512

f1:7b:af:4e:fa:ee cd:6:47:7:cc:e4 0.0.0.0.48051 > 0.0.0.0.20563: S 116556580:116556580(0) win 512

9c:d9:1c:b:7c:52 a6:1a:2f:12:13:91 0.0.0.0.60929 > 0.0.0.0.33052: S 16418121:16418121(0) win 512

27:c8:de:66:d8:6d b0:d9:79:44:6c:4 0.0.0.0.664 > 0.0.0.0.10745: S 1412924064:1412924064(0) win 512

fd:72:5a:60:79:21 ec:e6:a2:30:6c:e1 0.0.0.0.39865 > 0.0.0.0.49657: S 1061118039:1061118039(0) win 512

1f:a9:10:63:50:84 1d:19:30:5f:5:39 0.0.0.0.18769 > 0.0.0.0.33637: S 1299235605:1299235605(0) win 512

eb:b:8f:6c:8b:bf 48:c:25:31:a5:16 0.0.0.0.8981 > 0.0.0.0.18064: S 1503192924:1503192924(0) win 512

4c:8d:d8:61:4d:94 65:6f:0:2c:b3:86 0.0.0.0.22007 > 0.0.0.0.37235: S 1474792381:1474792381(0) win 512

f7:21:4c:15:d5:6f 43:8c:9a:6d:90:af 0.0.0.0.48890 > 0.0.0.0.29227: S 1261324152:1261324152(0) win 512

42:e0:7e:61:21:8b af:e6:5d:28:2d:ff 0.0.0.0.5674 > 0.0.0.0.17627: S 1523990207:1523990207(0) win 512

6:98:c1:26:ba:8 67:a:6:61:2e:5a 0.0.0.0.31705 > 0.0.0.0.25956: S 1519523848:1519523848(0) win 512

---

dentro de la consola de yakuake vemos como el atacante envía paquetes con direcciones

MAC aleatóreamente.

Paso 7: Vamos a cutecom y observamos que se muestran mensajes aceptando peticiones MAC.

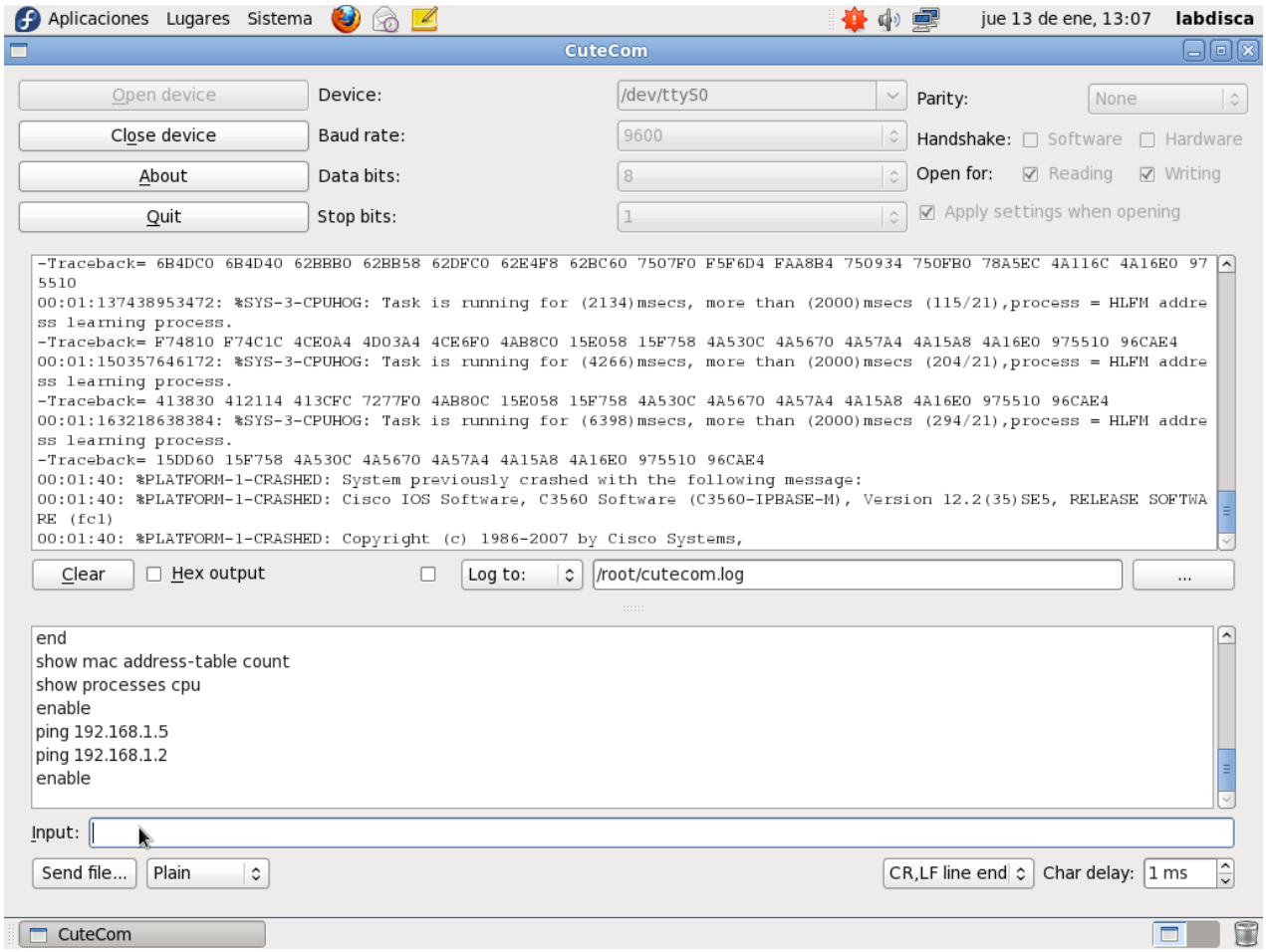


Figura 4.9: Paso 6: MAC flooding: Mensajes durante el ataque

Paso 8: Ahora vamos a ver que sucedido con nuestra tabla MAC para ello abrimos cutecom, en la figura 4.9 se muestran mensajes donde el switch continúa aprendiendo la nueva tabla cuando su tabla llega al límite de direcciones MAC colapsa. Ejecutamos el comando:

show MAC address-table count

Despues del ataque observamos en la tabla (figura 4.10) que las direcciones MAC dinamicas fuerón asignadas en su totalidad y el switch ya no acepta mas asociaciones por tanto este enviara por todos los puertos adquiriendo el comportamiento de un concentrador.

4.2. Práctica 2 (Mitigación Usando Port Security)

Paso 9: Ahora vamos a proteger todos los puertos de nuestro Switch usando Port security. Desde la terminal cutecom vamos a ejecutar los siguietes comandos.

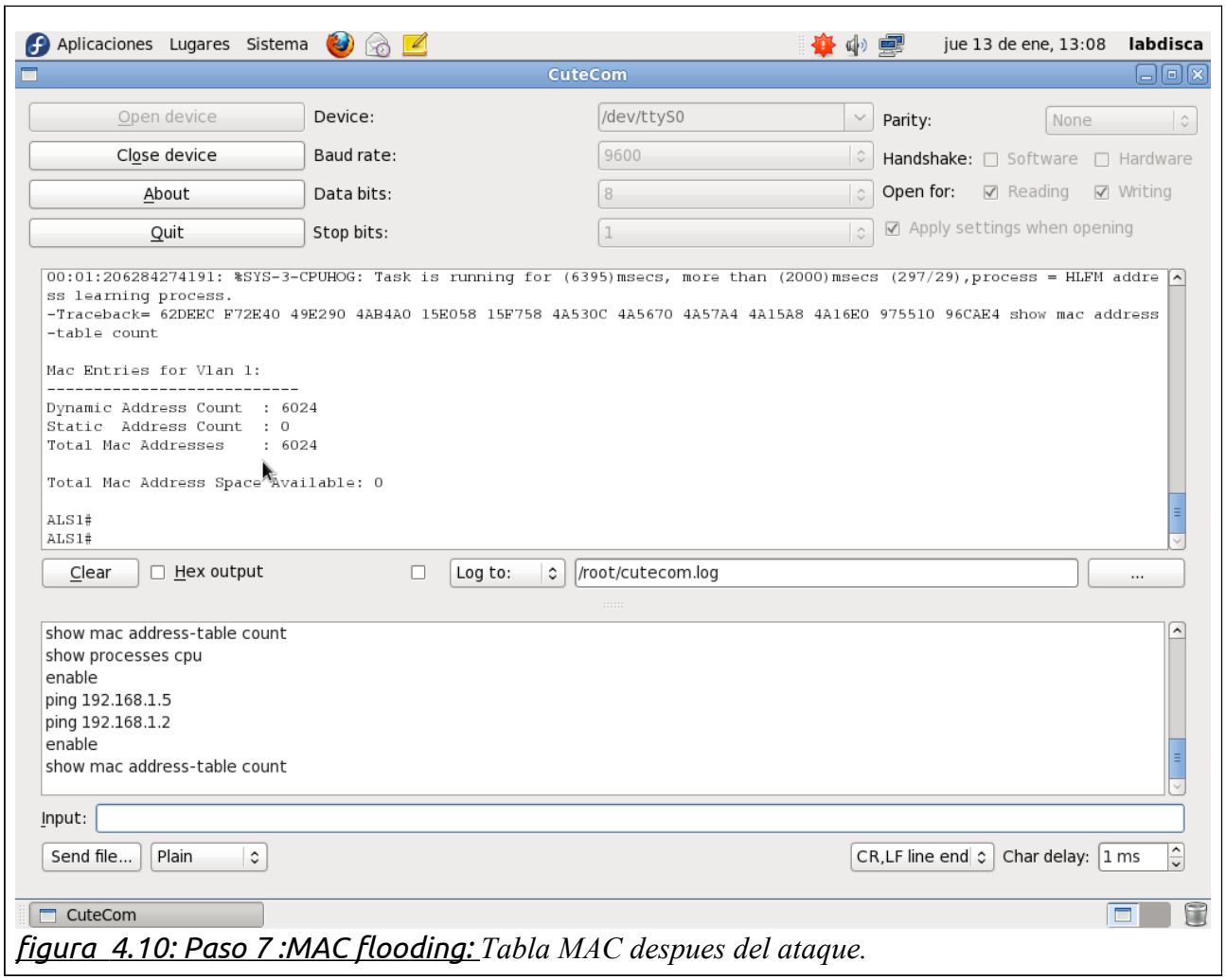


figura 4.10: Paso 7 :MAC flooding: Tabla MAC despues del ataque.

ALS1$ enable

ALS1# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

ALS1(config)#interface range fa0/1 – 10 (entramos al modo de configuración de los puertos 1 al 10)

ALS1(config-if-range)#switchport port-security

Command rejected: FastEthernet0/1 is a dynamic port.

Command rejected: FastEthernet0/2 is a dynamic port.

Command rejected: FastEthernet0/3 is a dynamic port.

Command rejected: FastEthernet0/4 is a dynamic port.

Command rejected: FastEthernet0/5 is a dynamic port.

Command rejected: FastEthernet0/6 is a dynamic port.

Command rejected: FastEthernet0/7 is a dynamic port.

Command rejected: FastEthernet0/8 is a dynamic port.

Command rejected: FastEthernet0/9 is a dynamic port.

Command rejected: FastEthernet0/10 is a dynamic port.

Esto quiere decir que el puerto no puede ser configurado como puerto seguro si se encuentra de forma dinámica, solo se puede cuando el puerto esta en modo "static acces[18]" o modo "trunk[19]".

ALS1(config-if-range)#switchport mode access

ALS1(config-if-range)#switchport port security

Si se ingresa solamente el comando básico, se asumen los valores por defecto: solo permite una dirección MAC en el puerto, que será la primera que se conecte al mismo, en caso de que otra dirección MAC intente conectarse utilizando el mismo puerto, este será deshabilitado o bloqueado. Claro esta que todos estos parámetros son modificables.

Switch(config-ig)#switchport port-security maximum [cantidad de MAC permitidas]

Esta opción permite definir el número de direcciones MAC que está permitido que se conecten a través de la interfaz del swtich. El número máximo de direcciones permitidas por puerto va desde 1 a 132. Es importante tener presente que este feature (rasgo) también limita la posibilidad de un ataque de seguridad por inundación de la tabla CAM (ver definiciones) del switch. El siguiente ejemplo ilustra la configuración sobre los de los puertos 1 al 10 para que solo acepten solo 1 direccion MAC como máxima posible.

ALS1(config-if-range)#switchport port-security maximum 1

Ettercap es 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.

ALS1(config-if)# switchport port-security violation [shutdown restrict protect]

Este comando establece la acción que tomará el switch en caso de que se supere el número de direcciones MAC que se establece con el comando anterior. Las opciones son deshabilitar el puerto, alertar al Administrador de la Red o permitir exclusivamente el tráfico de la MAC que se registró inicialmente.
En el siguiente ejemplo trabajando con los puerto 1 al 10 del switch, podemos especificar qué hacer si ese número de direcciones MAC es superado (por default deshabilitar el puerto)

Que deje de prender:

Switch(config-if)# switchport port-security violation protect

Que envíe alertas administrativas:

Switch(config-if)# switchport port-security violation restrict

18 ***Static access:****Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino.*

19 ***Modo Trunk****: Un enlace troncal permite que los usuarios de una misma Vlan en diferentes zonas puedan estar comunicados entre si, en este modo los usuarios pueden compartir informacion de la misma Vlan..*

Que deshabilite el puerto del switch:

Switch(config-if)# switchport port-security violation shutdown

Paso 10: Para nuestro caso vamos a hacer que el switch deshabilite el puerto cuando se presente el ataque.

ALS1(config-if)# switchport port-security violation shutdown

Posterior al haber deshabilitado el puerto del switch, este se puede volver habilitar con el siguiente comando previa autorización del Administrador de la Red:

Switch(config-if)# switchport port-security mac-address
Switch(config-if)# shutdown
Switch(config-if)# no shutdown

switchport port-security mac-address [MAC address]

Esta opción permite definir manualmente la dirección MAC que se permite conectar a través de ese puerto, o dejar que la aprenda dinámicamente varias direcciones MAC. Ejemplo:
ALS1(config)#interface range FastEthernet 0/1 - 10

(Dentro del modo configuración del puerto a configurar)

Switch(config-if)# switchport port-security mac-address sticky

(esta opcion leera y aprendera la primera mac-address que se conecte)

Switch(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx

(este comando te permitira definir una mac-address estatica) es decir:

1. Con la primera línea de comando le digo que agregue las MACs que va aprendiendo a la lista de MACs seguras.
2. Con la segunda linea de comando, que agregue la MAC xx:xx:xx:xx:xx a la lista de MACs seguras.
3. Si no agrego una segunda MAC, la primera MAC que escuche distinta a xx:xx:xx:xx:xx:xx será agregada a la lista de MACs seguras.

Atención..! Este comando no debe ser configurado en un puerto troncal o de backbone, ya que por estos puertos circulan tramas con múltiples direcciones MAC, diferentes de origen. Esto daría como resultaría el bloqueo del puerto.

Paso 10: A continuacion configuraremos los puertos del 1 al 10 para que el switch porteja sus puertos aprendiendo las direcciones MAC que se conecten:

ALS1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

ALS1(config)#interface range fa0/1 - 10

ALS1(config-if-range)#switchport port-security mac-address sticky

ALS1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

ALS1(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to down

ALS1(config-if-range)#

Paso 11: Ahora para que el switch aprenda las direcciones MAC de las terminales

conectadas vamos a hacer un ping a cada una de ellas.

ALS1#ping 192.168.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/3/5 ms

ALS1#ping 192.168.0.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.7, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/5/6 ms

ALS1#ping 192.168.0.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.5, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/6 ms

ALS1#

Paso 12: Ahora vamos a monitorizar el estado de los puertos.

ALS1#show port-security address

Secure Mac Address Table

Vlan	*Mac Address*	*Type*	*Ports*	*Remaining Age (mins)*
1	*0267.E422.11B4*	*SecureSticky*	*FastEthernet0/1*	*-*
1	*001E.683F.C8E0*	*SecureSticky*	*FastEthernet0/2*	*-*
1	*0800.E454.415B*	*SecureSticky*	*FastEthernet0/5*	*-*

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 6021

Ahora desde nuestra terminal donde haremos el ataque usando Yakuake vamos a dividir nuestra en 2 partes verticales para ello nos ubicamos en lo ue vamos a dividir.

Ingresamos a nuestra terminal yakuake (pulsando F12 por defecto).

Para dividir nuestra terminal usamos los siguientes comandos.

- Ctrl+Shift+T = División vertical

- Ctrl+Shift+L = División Horizontal
- Ctrl+Shift+R = Deshacer división (simplemente nos paramos en la ventana que queremos eliminar y pulsamos Ctrl+Shift+R)

Paso 13: Ahora nos paramos en la ventana de yakuake y pulsamos al mismo timepo Ctrl+Shift+L (Figura 4.11)

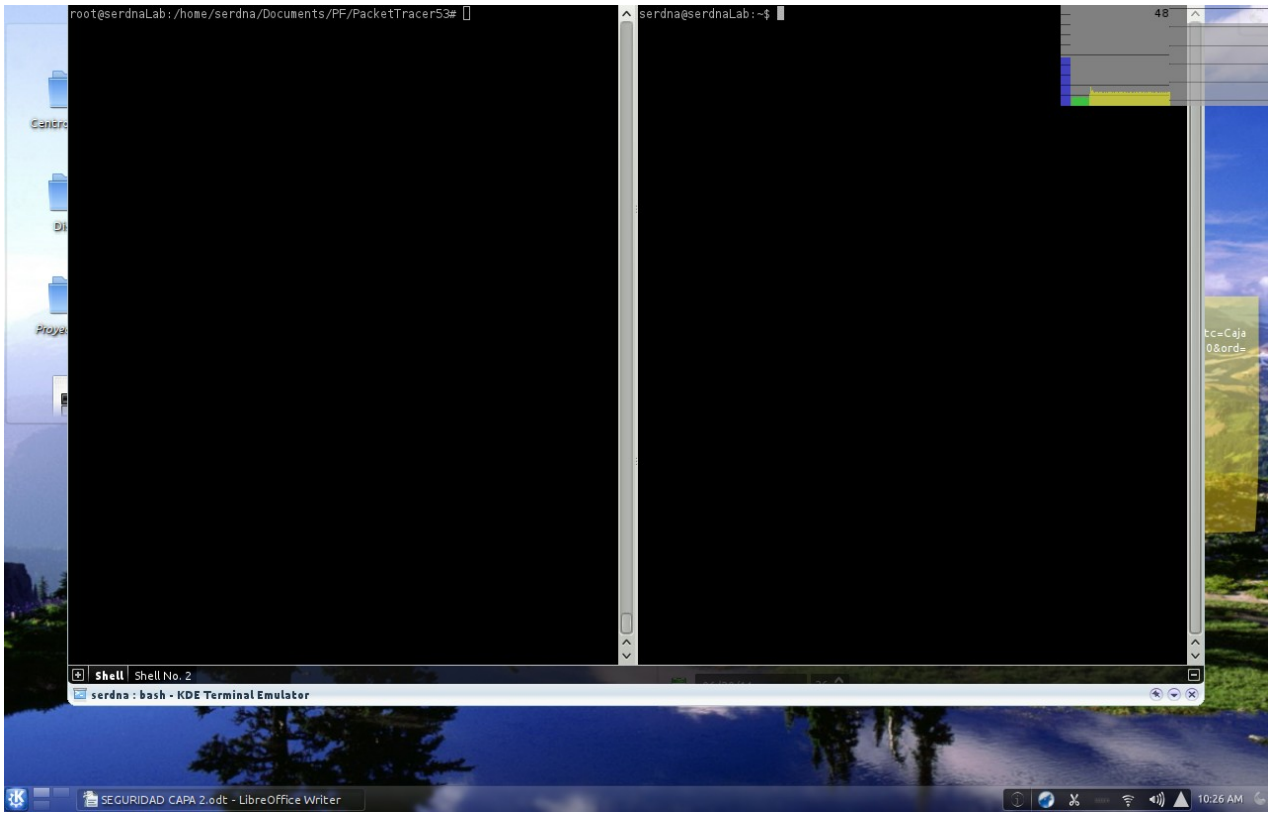


Figura 4.11: Paso 13: MAC Flooding: División Horizontal de Yakuake

Paso 14: Por un lado haremos ping al switch y por el otro lado efectuaremos el ataque con el comando macof -i [interfaz usada], y compararemos los resultados.

En la figura 4.12 observamos ue en el momento de realizar el ataque el switch desactiva el puerto, haciendo el destino inalcanzable para la terminal ue realiza el ataque.

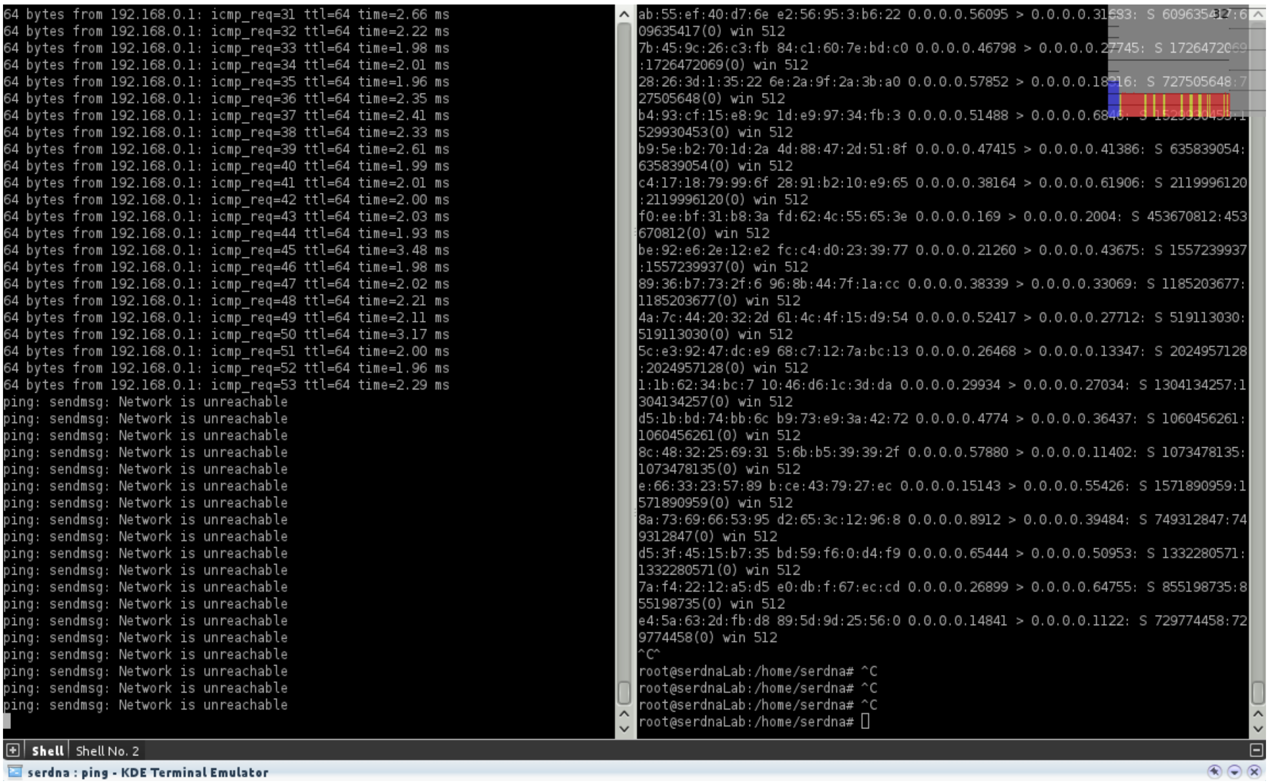


Figura 4.12: Paso 15: MAC Flooding: Ataque y ping simultaneos.

Paso 16: Ahora desde cutecomo hacemos un pIng a esta terminal...

ALS1>enable

ALS1#ping 192.168.0.7

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.7, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

Observamos que nuestro destino es inaccesible.
Paso 17: Ahora activamos el puerto desactivando y activando el puerto y verificamos haciendo ping a esta terminal nuevamente.

ALS1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

ALS1(config)#inter f0/2

ALS1(config-if)#shut

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

ALS1(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

ALS1(config-if)#end
ALS1#
%SYS-5-CONFIG_I: Configured from console by console

ALS1#ping 192.168.0.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/8 ms
---

4.3. Practica 3: Ataque ARP Spoofing

4.3.1. Escenario (figura 4.13)

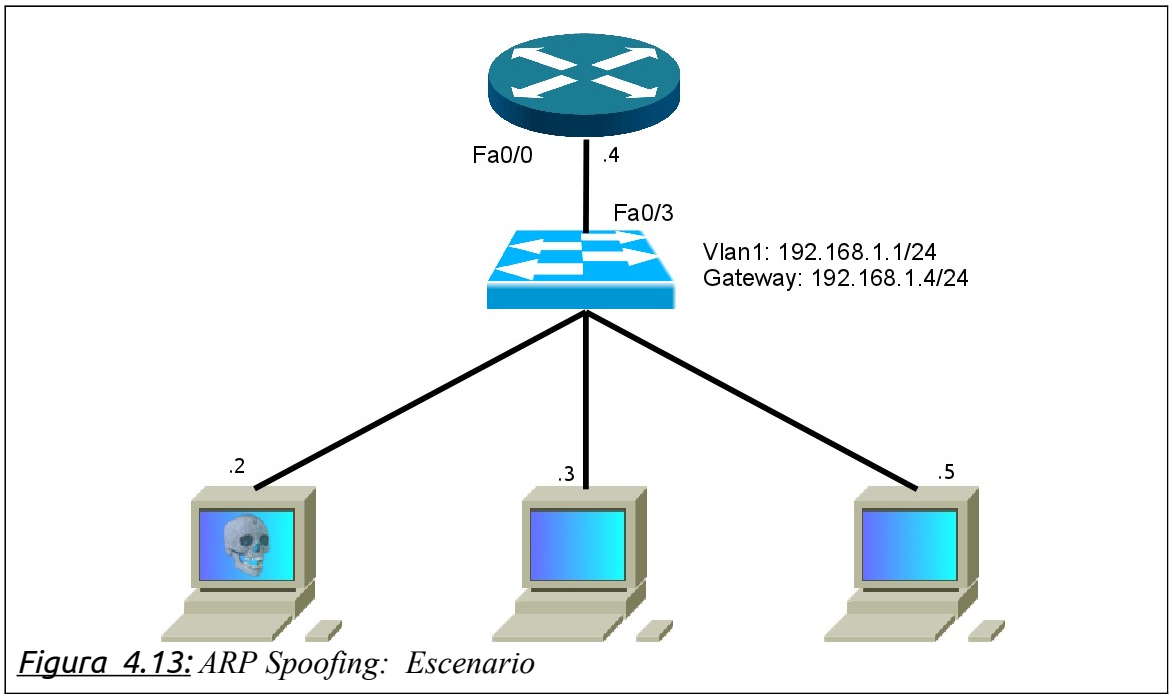


Figura 4.13: ARP Spoofing: Escenario

4.3.1.1. HERRAMIENTAS

4.3.1.1.1. Hardware

- Router Catalyst Cisco 2600 series.
- Switch Catalist Cisco 3560.
- 3 terminales con Fedora o Ubuntu.

4.3.1.1.2. Software

- Ettercap apt-get install ettercap-gtk.
- Cutecom.
- Yakuake.
- Wireshark.

Nota: El ettercap y el wireshark ambos son sniffer, pero vamos a usar uno como atacante y el otro como snnifer para hacer uso de diferentres herramientas.

4.3.1.2. ETTERCAP

Ettercap es 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.

4.3.1.2.1. **Funciones**

- Inyección de caracteres en una conexión establecida emulando comandos o respuestas mientras la conexión está activa.
- Compatibilidad con SSH1: puede interceptar users y passwords incluso en conexiones "seguras" con SSH.
- Compatibilidad con HTTPS: intercepta conexiones mediante http SSL (supuestamente seguras) incluso si se establecen a través de un proxy.
- Intercepta tráfico remoto mediante un túnel GRE: si la conexión se establece mediante un túnel GRE con un router Cisco, puede interceptarla y crear un ataque "Man in the Middle".
- "Man in the Middle" contra túneles PPTP (Point-to-Point Tunneling Protocol).
- Plataforma: Linux / Windows Ultima versión: NG-0.7.3

4.3.1.2.2. Soporte de Plug-ins

- Colector de contraseñas en: Telnet, FTP, POP, Rlogin, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, Napster, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, Half-Life, Quake3, MSN, YMSG.
- Filtrado y sustitución de paquetes.
- OS fingerprint: es decir, detección del sistema operativo remoto.
- Mata conexiones.
- Escaner de LAN: hosts, puertos abiertos, servicios...

- Busca otros envenenamientos en la misma red.
- Port Stealing (robo de puertos): es un nuevo método para el sniff en redes con switch, sin envenenamiento ARP".

Ettercap nos propone dos modos, el por defecto (unified sniff) o el bridged sniff, unos siendo interactivo y el otro no.

Una vez que empieza a rastrear el tráfico, obtendrás un listado de todas las conexiones activas, junto a una serie de atributos acerca de su estado (active, idle, killed, etc.). El asterisco indica que una contraseña fue recogida en esa conexión.

4.3.1.2.3. Instalación

Como root desde yakuake tipeamos el comando:
[root@labdiscaxx ~]# **yum install** ettercap-gtk

4.3.1.3. WIRESHAK

Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

4.3.1.4. CONFIGURACIÓN DEL GATEWAY

4.3.1.4.1. Configuración del Switch

¡Importante!
Paso 1: Limpiamos la configuración tanto del switch como del router. Anexos "Limpiando la configuración del Router/ Switch".

Paso 2: Configuración del Switch.
ALS1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

ALS1(config-if)#inter vlan 1

ALS1(config-if)#ip add 192.168.1.1 255.255.255.0

ALS1(config-if)#no shut

ALS1(config-if)#ip default-gateway 192.168.1.4

ALS1(config)#end

ALS1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

ALS1(config)#interface FastEthernet 0/4

ALS1(config-if)#switchport trunk encapsulation dot1q

ALS1(config-if)#switchport mode trunk

00:25:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down

00:25:31: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

ALS1(config-if)#end

Paso 3: Configuración del Router

Router(config)#hostname Gateway

Gateway(config)#inter Fastethernet 0/0

Gateway(config-if)#no shut

Gateway(config-if)#

Gateway(config-if)#

**Dec 29 10:02:20.563: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up*

**Dec 29 10:02:21.563: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to upinterface ethernet 0/0.1*

Gateway(config)#interface fastethernet 0/0.1

Gateway(config-subif)#description management VLAN 1

Gateway(config-subif)#encapsulation dot1q 1 native

If the interface doesn't support baby giant frames

maximum mtu of the interface has to be reduced by 4

bytes on both sides of the connection to properly

transmit or receive large packets. Please refer to

documentation on configuring IEEE 802.1Q vLANs.

**Dec 29 10:06:05.087: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up*

Gateway(config-subif)#ip add 192.168.1.4 255.255.255.0

Gateway(config-subif)#end

Paso 4: Monitoreo de la configuración de los puertos del router.

El comando “show ip interface brief” nos muestra el resumen de la configuración de los puertos del dispositivo de capa 3.

Gateway# show ip interface brief

Interface	*IP-Address*	*OK? Method Status*	*Protocol*
FastEthernet0/0	*unassigned*	*YES unset up*	*up*
FastEthernet0/0.1	*192.168.1.4*	*YES manual up*	*up*
FastEthernet0/1	*unassigned*	*YES unset administratively down*	*down*
FastEthernet0/1/0	*unassigned*	*YES unset up*	*down*
FastEthernet0/1/1	*unassigned*	*YES unset up*	*down*
FastEthernet0/1/2	*unassigned*	*YES unset up*	*down*
FastEthernet0/1/3	*unassigned*	*YES unset up*	*down*
Serial0/0/0	*unassigned*	*YES unset administratively down*	*down*
Vlan1	*unassigned*	*YES unset up*	*down*

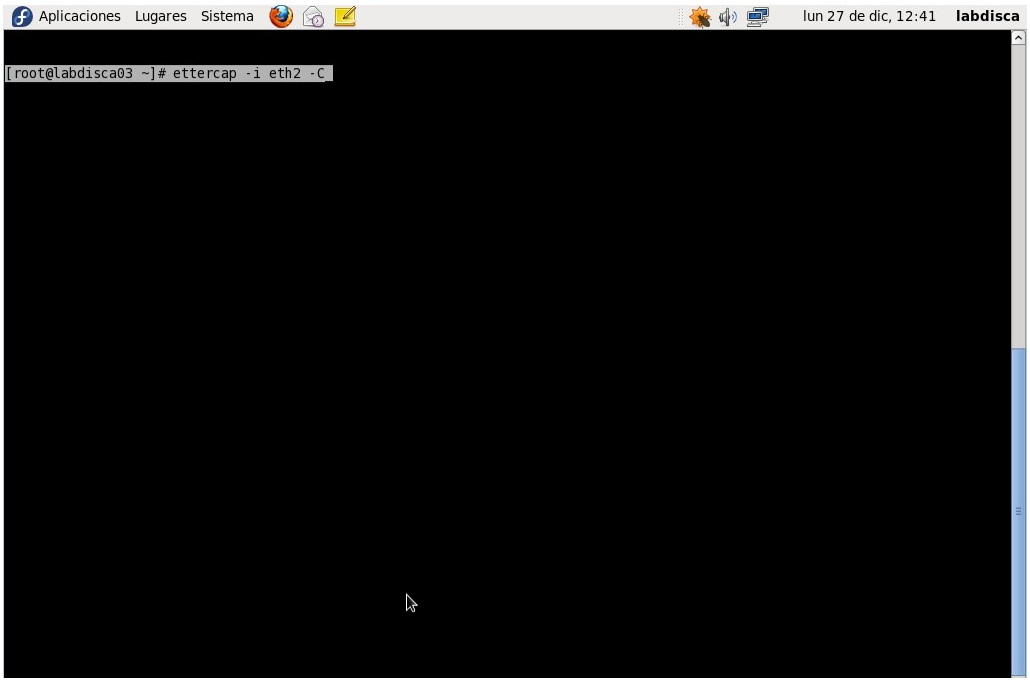


Figura 4.14: Paso 7: ARP Spoofing: Ejecutando Ettercap desde yakuake

Paso 5: Guardamos la configuración...

Gateway#copy running-config startup-config

Comprobamos la configuración entre el Switch y el router...

ALS1#ping 192.168.1.4

Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:

!!!!!

Paso 6: Guardamos nuestra configuración....

ALS1#copy running-config startup-config

4.3.1.5. INICIANDO EL ATAQUE

Paso 6: Desde yakuake (lo abrimos pulsando F12 por defecto) digitamos el comando:

root@labdisca03 ~]# ettercap -i eth2 -C (Figura 4.14)

Paso 7: En el menú sniff de ettercap seleccionamos "unified sniffing".

En el menú Sniff nos muestra 2 métodos para esnifar: (figura 4.15)

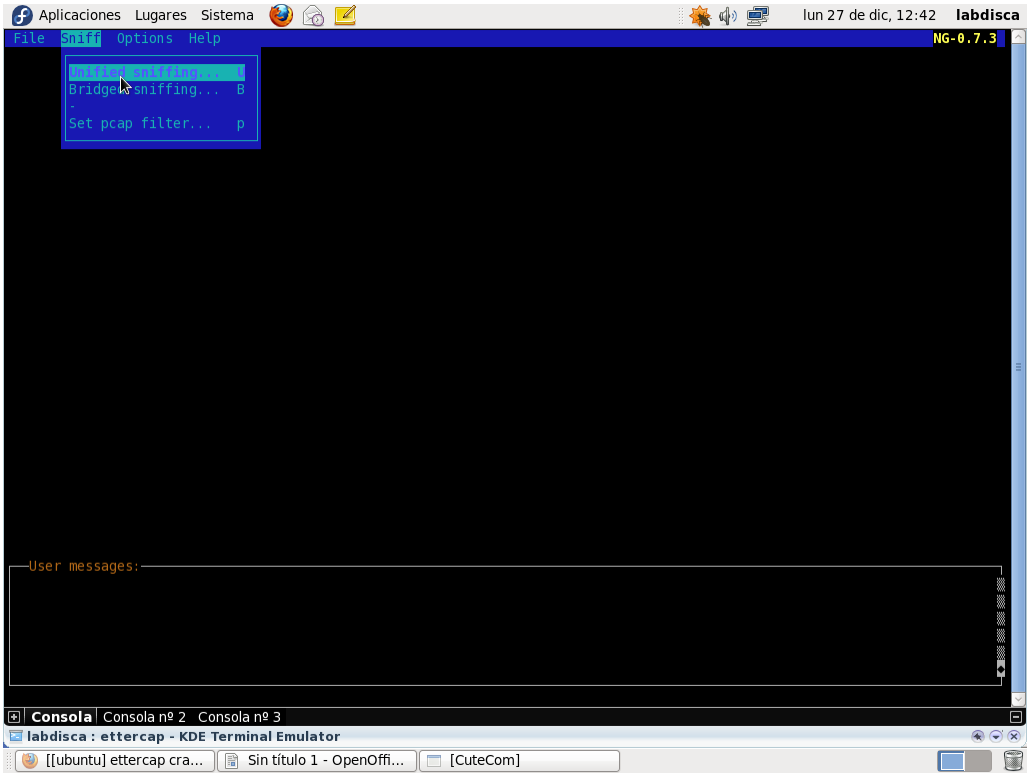


Figura 4.15: Paso 8: ARP Spoofing: Seleccionando "Unified Sniffing"

UNIFIED SNIFF: Este método esnifa todos los paquetes qque pasan en el cable de red. Usted puede seleccionar entre colocar o no la targeta en modo primiscuo (Opción -p). El paquete no se dirige al host que está ejecutando ettercap será enviado automáticamente usando la capa 3 de enrrutamiento. Además usted puede lanzar un ataque MITM con una herramienta diferente y deja a ettercap modificar los paquetes y enviarlos nuevamente para usted.

El kernel de envio de ip está siempre desabilitado en ettercap. Esta hecho para prevenir enviar un paquete 2 veces (uno por ettercap y otro por el kernel[20]). Este es un comportamiento invasivo de los gateways. Por eso se recomienda usar ettercap solo en los gateways con el modo UNOFFENSIVE MODE ENABLE. Desde que ettercap escuche solo por un puerto, enviada en el gateway en modo ofensivo, no permite que los pauetes retornen al segundo puerto.

BRIDGE. Este usa dos puertos de red envía el tráfico del uno al otro mientras esnifa y hace filtrado de contenido. Este metodo de esifer es totalmente cauteloso por lo ue no hay manera de encontrar a alguien en medio del cable. Usted puede ver este método como un ataque MITM a la capa 1. Usted estaría en la mitad del cable entre 2 entidades. No use este modo en gateways o transformará este gateway en un Bridge.

Nota: Usted puede usar el motor de filtrado de contenido, para descartar paquetes que no podrían pasar. Este modo ettercap trabajará como un IPS [21]en linea.

Paso 9: Selecionamos el puerto que queremos atacar en este caso nuestro puerto fisica es eth2. (Figura 4.16)

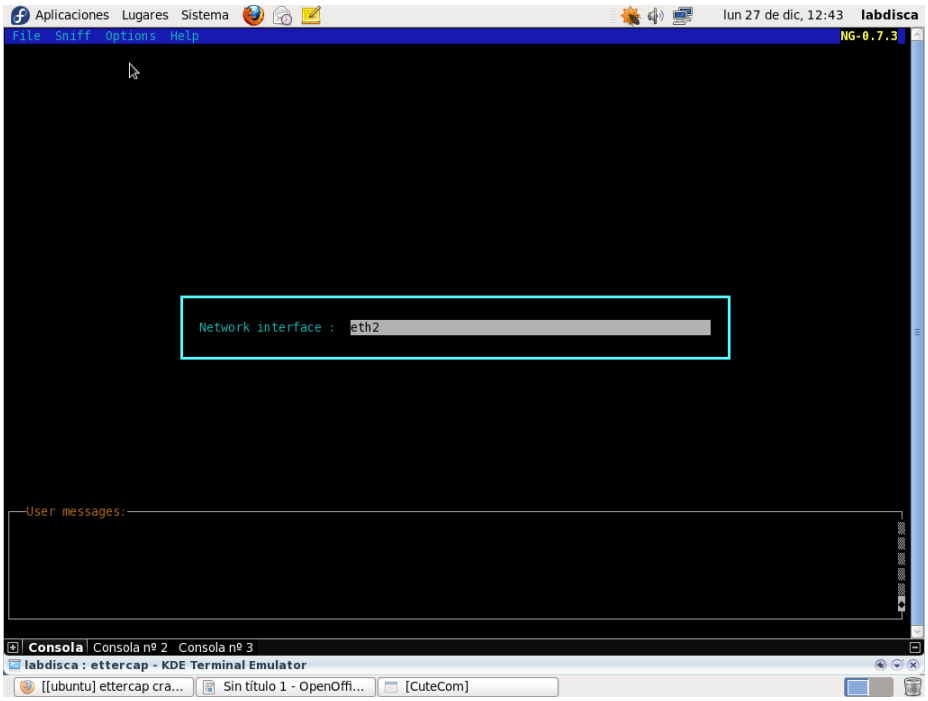


Figura 4.16: Paso 9: ARP Spoofing: Elección del puerto

Paso 10: Dentro del menú host selecionamos scan for host. (Busca las terminales activas en la red) Figura 4.17

20 *En informática, un núcleo o kernel (de la raíz germánica Kern) es un software que constituye la parte más importante del sistema operativo.1 Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.*

21 *Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.*

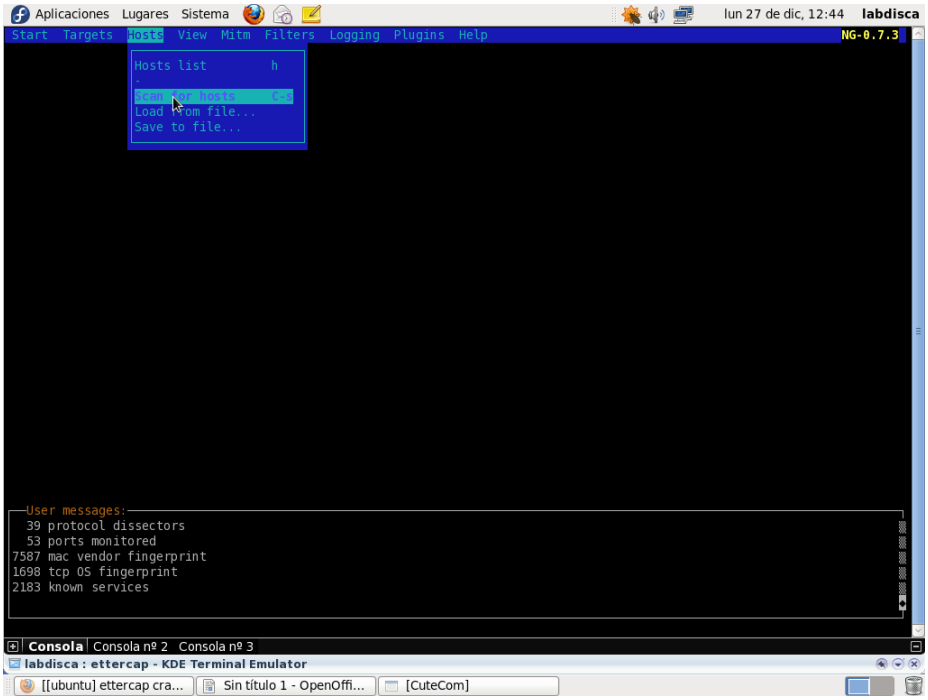


Figura 4.17: Paso 10: ARP Spoofing: Escanear terminales activas

Paso 11: Dentro del menú host selecionamos ahora "host list". (Lista las terminales activas en la red). En la parte inferior nos muestra que se han encontrado 4 terminales activas, (Figura 4.18)

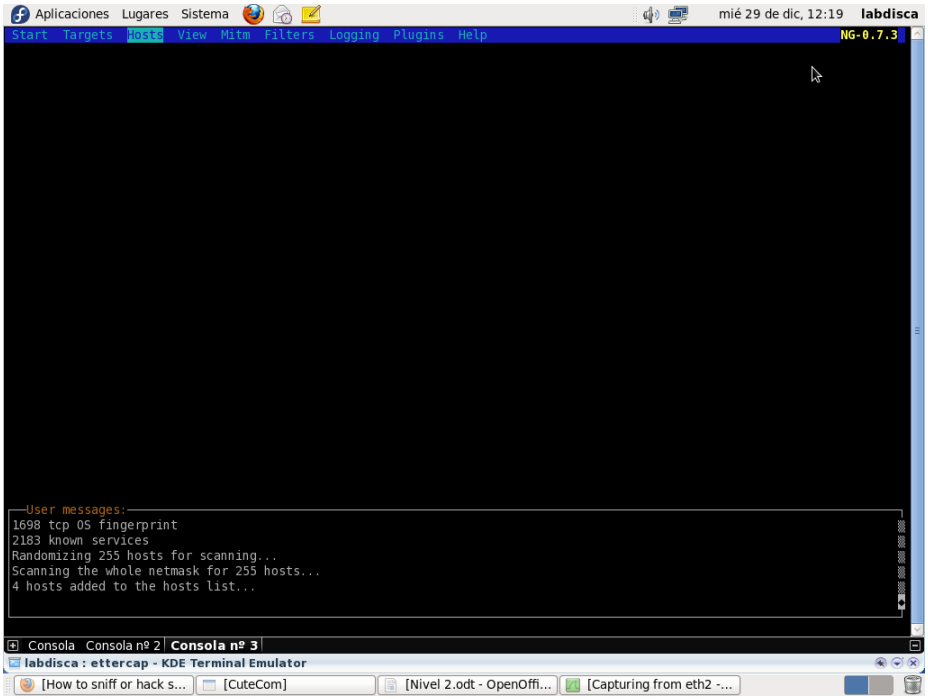


Figura 4.18: Paso 11: ARP Spoofing: Terminales encontradas

Paso 12: Seleccionamos la vlan 1 192.168.1.1 y pulsamos 1 (Primer objetivo) y seleccionamos la terminal 192.168.1.3 y pulsamos 2 (segundo objetivo) (Figura 4.19).

Ahora nuestro switch quedo en el objetivo 1 y nuestro host esta en el objetivo 2. Si no elegimos segundo objetivo el monitoreara todas las terminales conectadas al primer objetivo esea el switch.

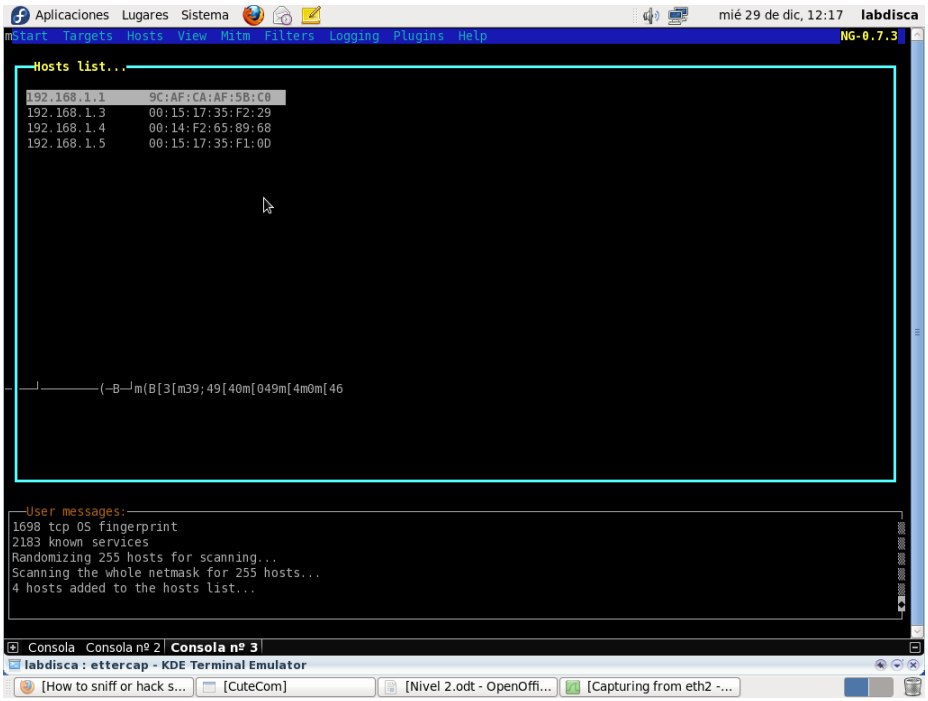


Figura 4.19: Paso 11: ARP Spoofing: Eligiendo objetivos de ataque

Paso 13: Vamos al menu Targets y hacemos click en Current targets (objetivos Actuales). Este nos mostrará cada objetivo en 2 recuadros separados (Figura 4.20) llamados targets (objetivos).
Desde la terminal cpon la IP 192.168.1.3 abrimos yakuake y hacemos ping a 192.168.1.4
Antes de continuar nuestro ataque analizaremos los paquetes con wireshark

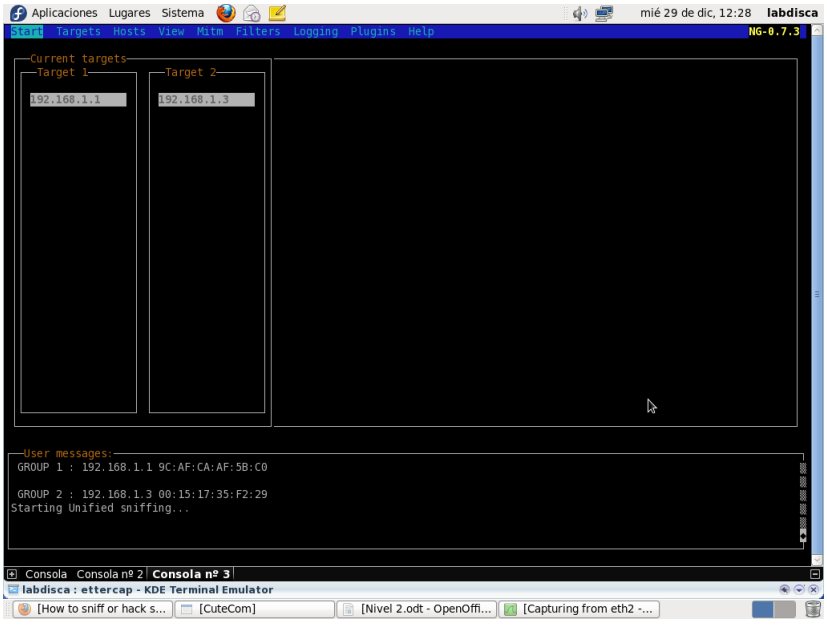


Figura4.20: Paso 13: ARP Spoofing: Objetivos actuales

Paso 14: Para el analisis de paquetes usaremos wireshark. Para ejecutar wireshark, abrimos una sesión nueva en yakuake para continuar con nuestra sesi{on de ettercap haciendo un click sobre (+) parte inferior izuierda de la ventana de yakuake. Figura 4.21

Figura 4.21: Nueva sesión

Para cambiar de sesión hacemos un click derecho sobre las pestañas shell een este caso nuestra nueva sesión estara en “shell N° 2” y la sesión de ettercap estará en la sesión “shell”. (Figura 4.22)

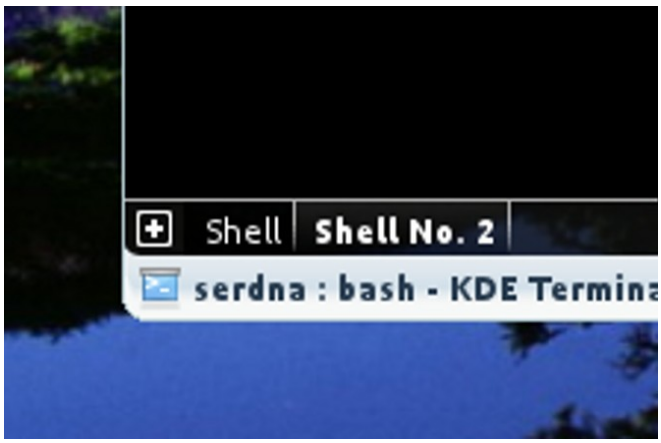


figura 4.22: Yakuake:Varias sesiones en yakuake

Para cerrar las sesiones solamente hacemos un click derecho en el (-) en la parte inferior derecha de la ventana de yakuake. Se cerrara la sesión que esté activa.

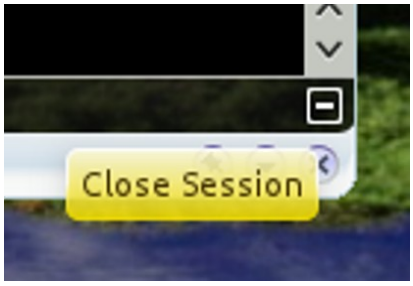


Figura4.23: Yakuake: Cerrar sesión

Debemos tener cuidado de estar ubicados en la sesión que vamos a cerrar si no cerraremos la sesion incorrecta y perderemos lo que estemos haciendoen este caso perdiamos el progreso que llevemos con ettercap y tendriamos que repetirlo hasta este paso

Ahora monitorearemos paquetes con wireshark, abrimos yakuake y entramos como root ya que las interfaces solo son mostradas como administrador.

Paso 15: Ingresamos el comando
[root@labdisca04 ~]# wireshark

En la ventana principal de wireshark podemos ver los puertos que tenemos disponibles:

- eth2.
- eth3.
- 4 puertos USB.
- lo = Loopback.

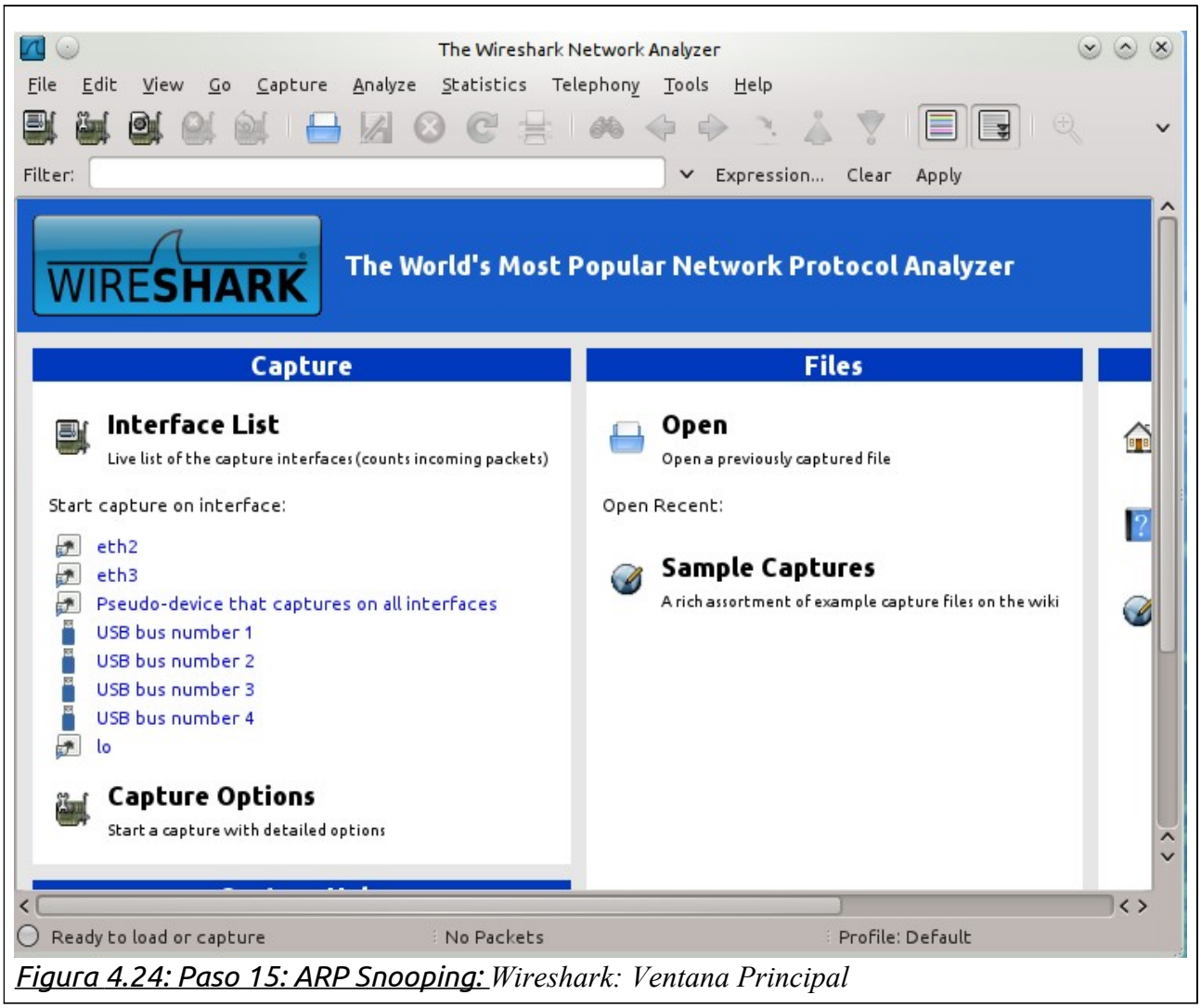


Figura 4.24: Paso 15: ARP Snooping: Wireshark: Ventana Principal

Paso 16: Elegimos eth2. Comienza el monitoreo de paquetes.

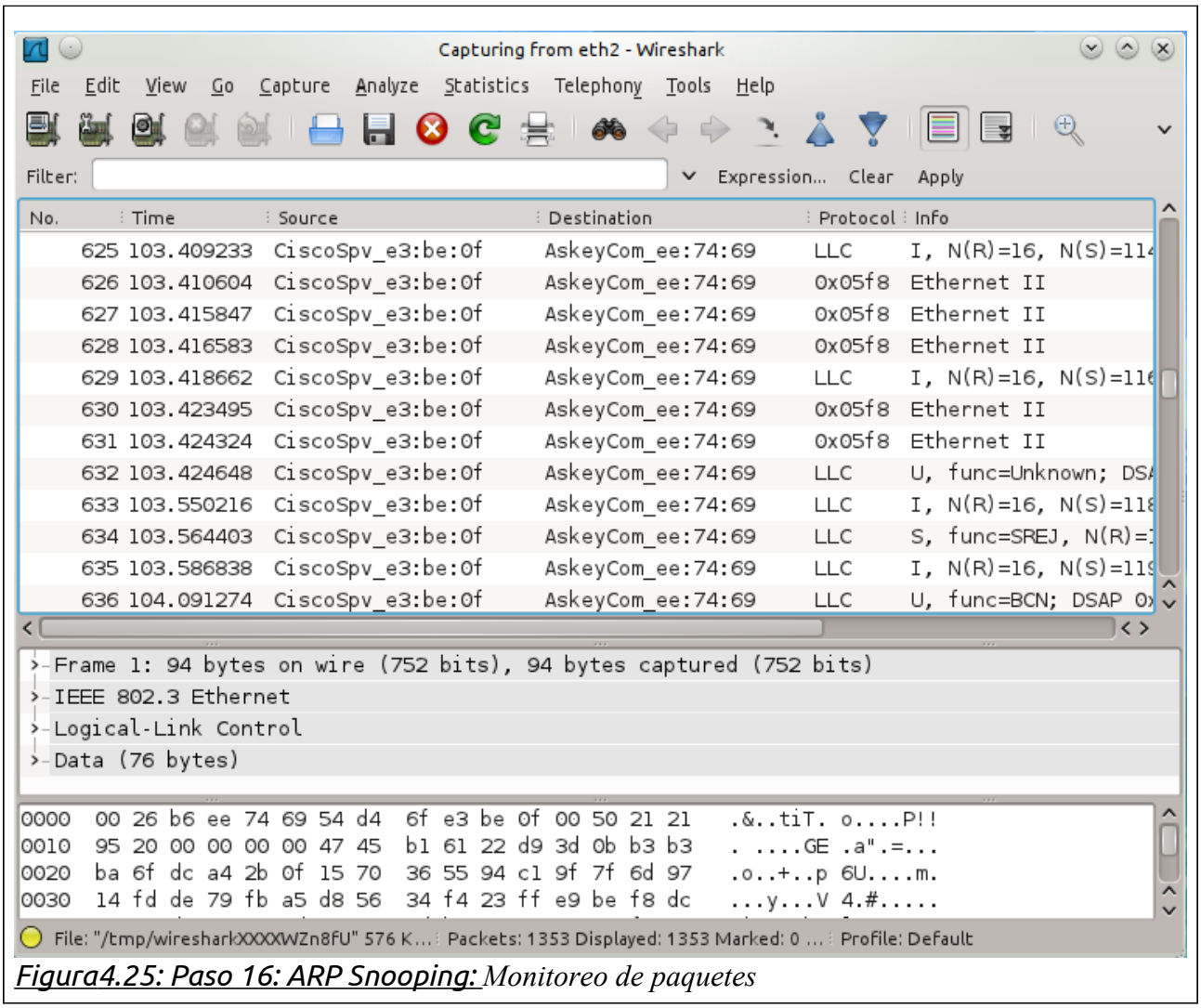


Figura4.25: Paso 16: ARP Snooping: Monitoreo de paquetes

Volvemos a yakuake vamos a la sesión de ettercap.

Paso 17: A continuación vamos al menú MITM, Seleccionamos el ataque arp poisoning. (figura 4.26)

En el recuadro parameters escribimos remote para conexiones remotas y nos permitirá conocer todas las conexiones que entran y salen del switch.

Ha comenzado nuestro ataque arp ahora todas las peticiones arp pasarán por el atacante, tomando el lugar del gateway. Esto hara que todos los paquetes cruzen por el terminal atacante. Como observaremos en la siguiente figura 4.25.

Paso 18: Volvemos a wireshark y observamos que empezo con una captura de paquetes. (Figura 4.27)

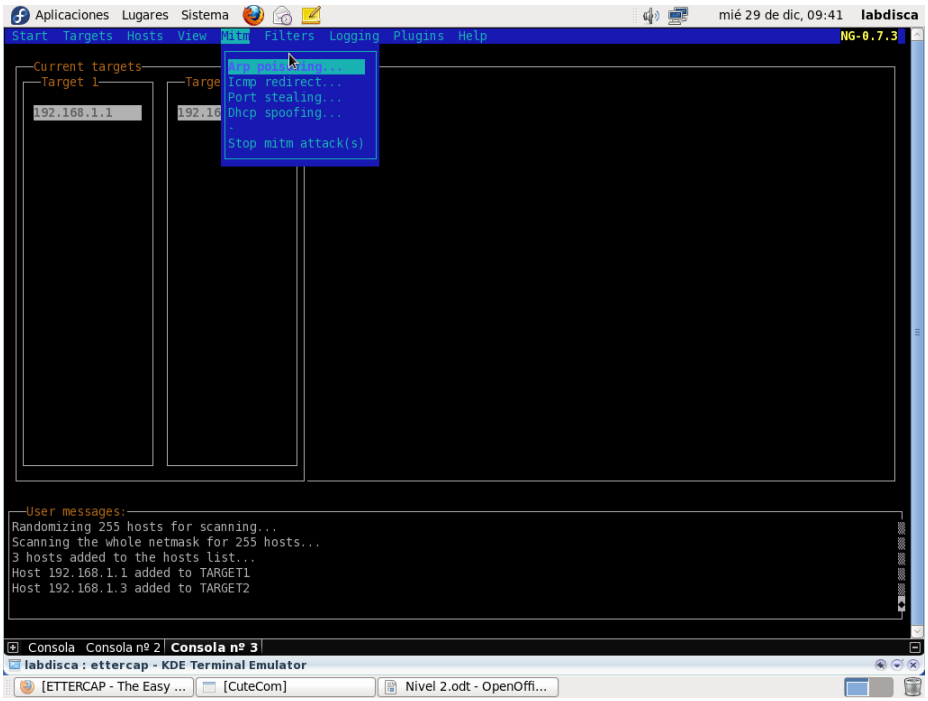


Figura 4.26: Paso 17: ARP Snooping: Iniciando el ataque

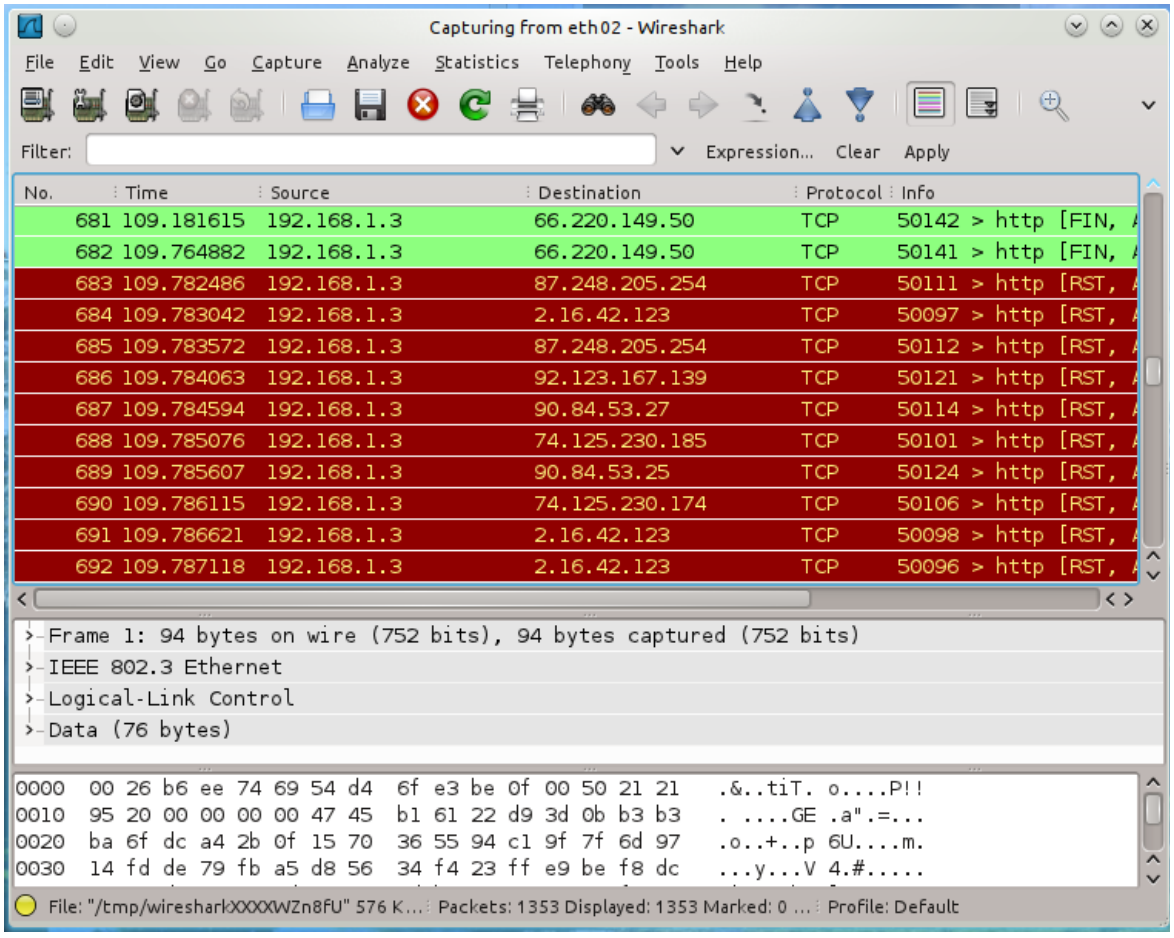


Figura 4.27: Paso 18: ARP Snooping: Captura de paquetes:

4.4. Práctica 4: Mitigando Ataques Arp Usando DHCP Snooping.

Paso 19: Limpiamos la configuración tanto del switch como del router. Anexos "Limpiando la configuración del Router/ Switch"

Paso 20: Abrimos cutecom desde yakuake como root y accedemos al switch. Digitamos los siguientes comandos:

```
ALS1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#ip dhcp snooping
ALS1(config)#ip arp inspection vlan 1
% Incomplete command.

ALS1(config)#
ALS1(config)#interface fa 0/2
ALS1(config-if)#
ALS1(config-if)#ip dhcp snooping trust
ALS1(config-if)#
ALS1(config-if)#ip arp inspection trust
ALS1(config-if)#
ALS1(config-if)#end
ALS1#
```

Y esto es lo que se observaría desde desde la misma terminal cutecom...

```
01:09:29: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 1.
([0015.1735.f10e/192.168.1.3/9caf.caaf.5bc0/192.168.1.1/01:09:29 UTC Mon Mar 1
1993])
01:09:29: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 1.
([0015.1735.f10e/192.168.1.1/0015.1735.f229/192.168.1.3/01:09:29 UTC Mon Mar 1
1993])
01:09:39: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 1.
([0015.1735.f10e/192.168.1.3/9caf.caaf.5bc0/192.168.1.1/01:09:39 UTC Mon Mar 1
1993])
01:09:39: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 1.
([0015.1735.f10e/192.168.1.1/0015.1735.f229/192.168.1.3/01:09:39 UTC Mon Mar 1
1993])
01:09:49: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 1.
([0015.1735.f10e/192.168.1.3/9caf.caaf.5bc0/192.168.1.1/01:09:49 UTC Mon Mar 1
1993])
01:09:49: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 1.
([0015.1735.f10e/192.168.1.1/0015.1735.f229/192.168.1.3/01:09:49 UTC Mon Mar 1
1993])inter fa 0/3

01:09:59: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 1.
([0015.1735.f10e/192.168.1.3/9caf.caaf.5bc0/192.168.1.1/01:09:59 UTC Mon Mar 1
1993])
01:09:59: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 1.
([0015.1735.f10e/192.168.1.1/0015.1735.f229/192.168.1.3/01:09:59 UTC Mon Mar 1
```

1993])
01:10:10: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 1. ([0015.1735.f10e/192.168.1.3/9caf.caaf.5bc0/192.168.1.1/01:10:09 UTC Mon Mar 1 1993])
01:10:10: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 1. ([0015.1735.f10e/192.168.1.1/0015.1735.f229/192.168.1.3/01:10:09 UTC Mon Mar 1 1993])ip arp inspection trust

4.4.1. DHCP Snooping

DHCP snooping es una función de seguridad que provee seguridad por filtración de mensajes DHP no confiables por creación y mantenimiento de una tabla DHCP snooping. Un mensaje no confiable es un mensaje que se recibe desde afuera de la red o del cortafuegos y que puede causar un ataques de tráfico dentro de la red.

La tabla ligada DHCP snooping binding table contiene direciones MAC, direcciones IP, tiempo de permiso, tipo de unión o ligadura, número de VLAN y puerto de información que corresponde a los puertos locales de un switch no confiables; este no contiene información referente a los host interconectados con puerto no confiable[22]. Un puerto no confiable es un puerto que es configurado para recibir mensajes de afuera de la red o del cortafuegos

The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCP snooping actúa como un cortafuegos entre los puertos no confables de las terminales y el servidor DHCP. Tambien da una forma para diferenciar entre Puertos no confiables conectados al usaurio final y los puertos confiables conectados a un servidor DHCP u otro switch.

22 *Untrusted en ingles*

4.5. Práctica 5: Ataque DHCP STARVATION (Agotamiento De Direcciones).

4.5.1. Esceneario

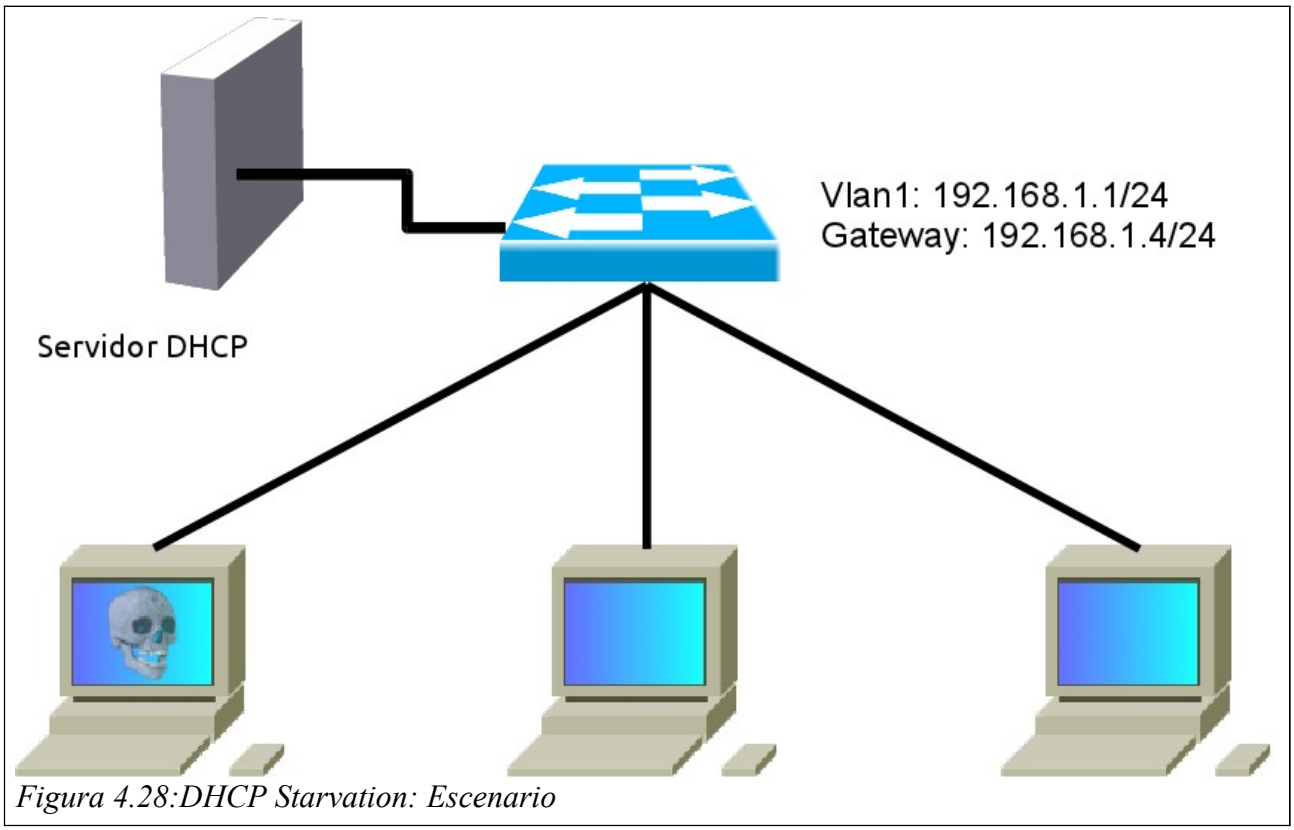


Figura 4.28:DHCP Starvation: Escenario

4.5.1.1. DESCRIPCIÓN

DHCP starvation es un ataque que consiste en inundar con peticiones DHCP_REQUEST al servidor DHCP, con direcciones MAC falseadas y con el objetivo de agotar su espacio de direcciones asignables. El objetivo es que el servidor DHCP no sea capaz de responder a otros clientes y así realizar otro tipo de ataques (DHCP rogue).

4.5.1.2. HERRAMIENTAS

4.5.1.2.1. Hardware

- Clavister Secure 50 series. Servidor DHCP
- 3 host configuración IP dinámica.
- 1 switch catalys cisco 3560

4.5.1.2.2. Software

- Yersinia
- Cutecom
- Yakuake

4.5.1.2.3. Yersinia

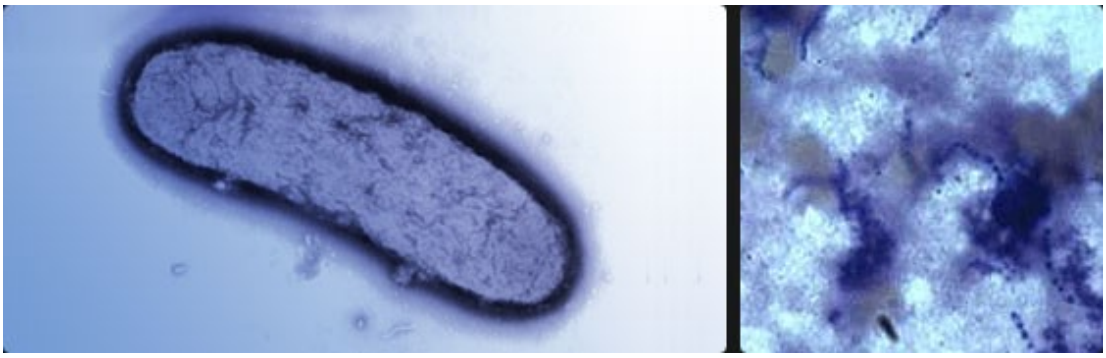


Figura 4.29: Yersinia

Yersinia es una herramienta de red diseñada para tomar ventaja de algunas debilidades en los diferentes protocolos de red. Pretende ser un framework sólido para analizar y probar redes y sistemas.

En la actualidad, hay algunos protocolos de red implementado, pero otros estan por venir . Los ataques de los siguientes protocolos de red se pueden implementar .

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

4.5.1.2.3.1. INSTALACIÓN

Ingresamos a Yakuake (Pulsamos F12 por defecto)
Para Fedora:
yum install yersinia

Para Ubuntu:
apt-get install yersinia

4.5.1.3. CONFIGURACIÓN DE LA IP DINÁMICA

Una vez conectado y configurado el servidor DHCP al Switch procedemos a la configutación de la IP dinámica en cada una de las terminales.

Paso 1: Hacemos click derecho sobre el icono de conexiones de red y selecionamos Editar las conexiones. (Figura 4.30)

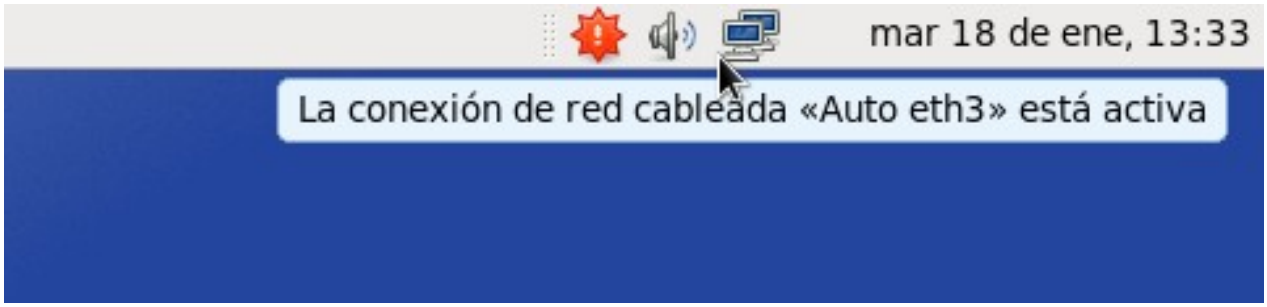


Figura 4.30:Paso 1: DHCP Starvation:Conexiones de red

Paso 2: En la ventana de coneciones de red selecionamos nuestro puerto que esta conectada al Swith en este caso eth3 y la editamos. (Figura 4.31)

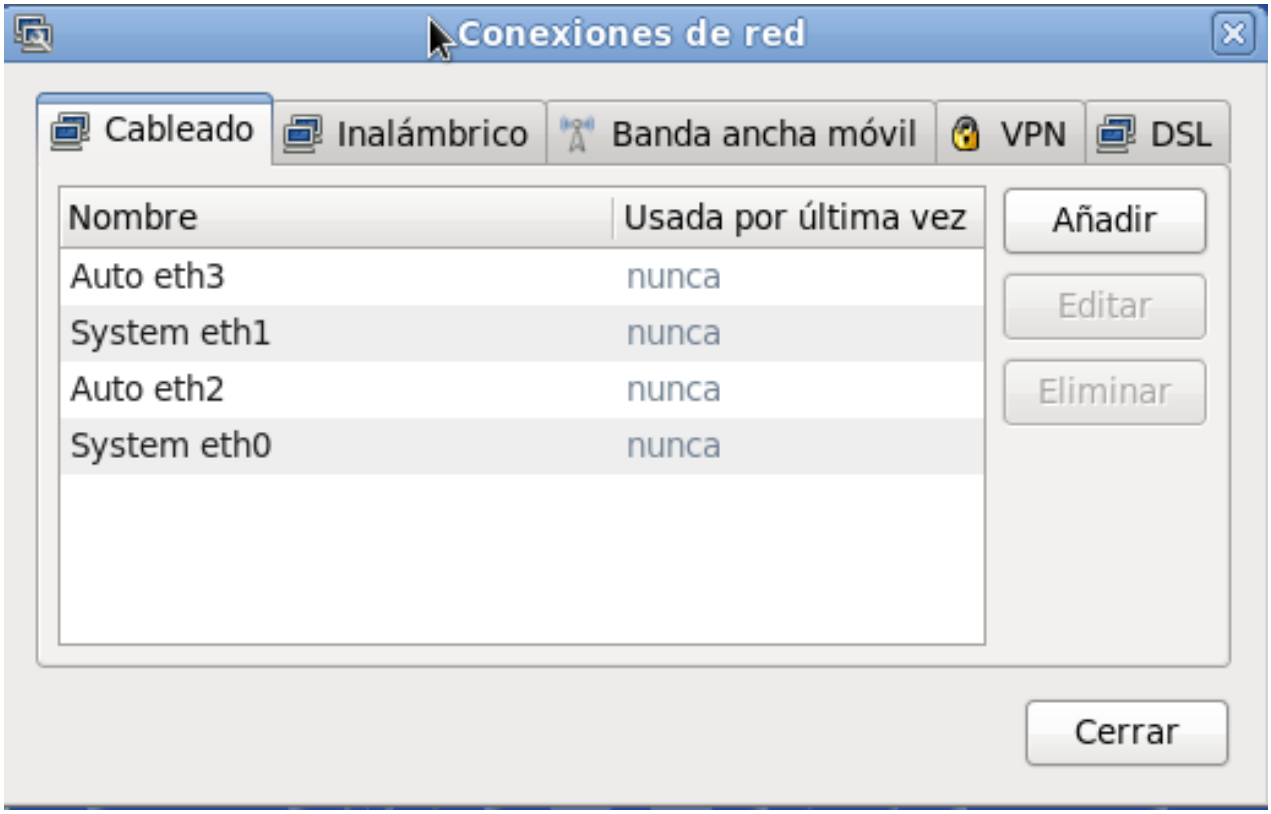


Figura 4.31: Paso 2: DHCP Starvation:Configuración del puerto:Elección del puerto

Paso 3: En ajustes de Ipv4 selecionamos Método - Automático (DHCP) (figura 4.32)

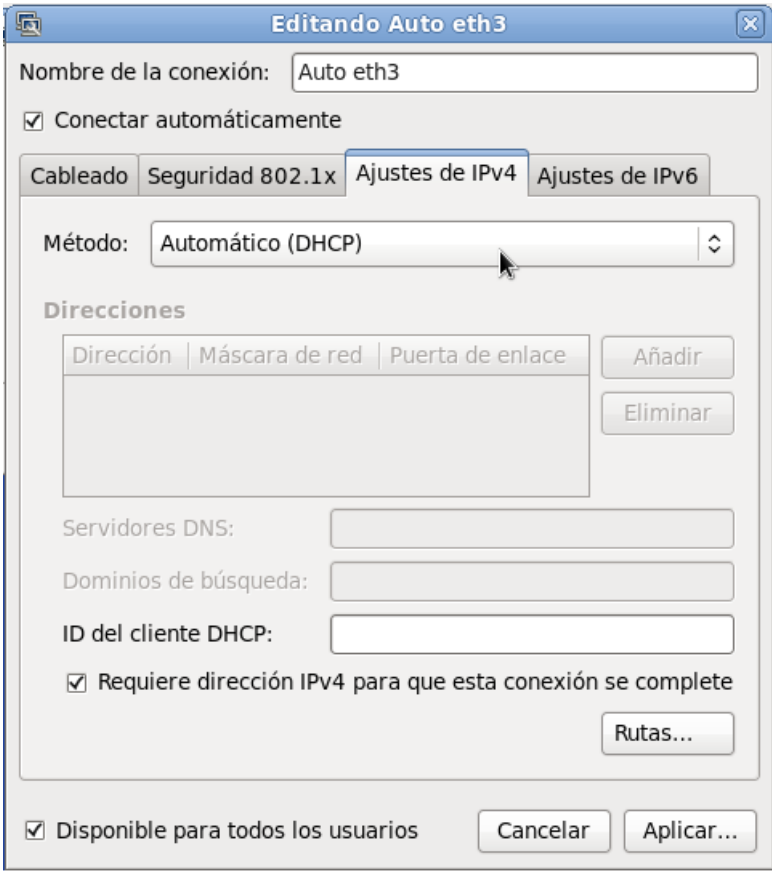


Figura 4.32: Paso 3: DHCP Starvation: Editando configuración IP del puerto

Paso 4: Hacemos click en Aplicar introducimos contraseña de administrador y cerramos conexiones de red. Revisamos configuración. (Figura 4.33)

Figura 4.33: Paso 4: DHCP Starvation:Resultado de la configuración

4.5.2. DHCP Starvation Con Yersinia

Paso 5: Ejecutamos yersinia con digitando el comando yersinia -I. (Figura 4.34)

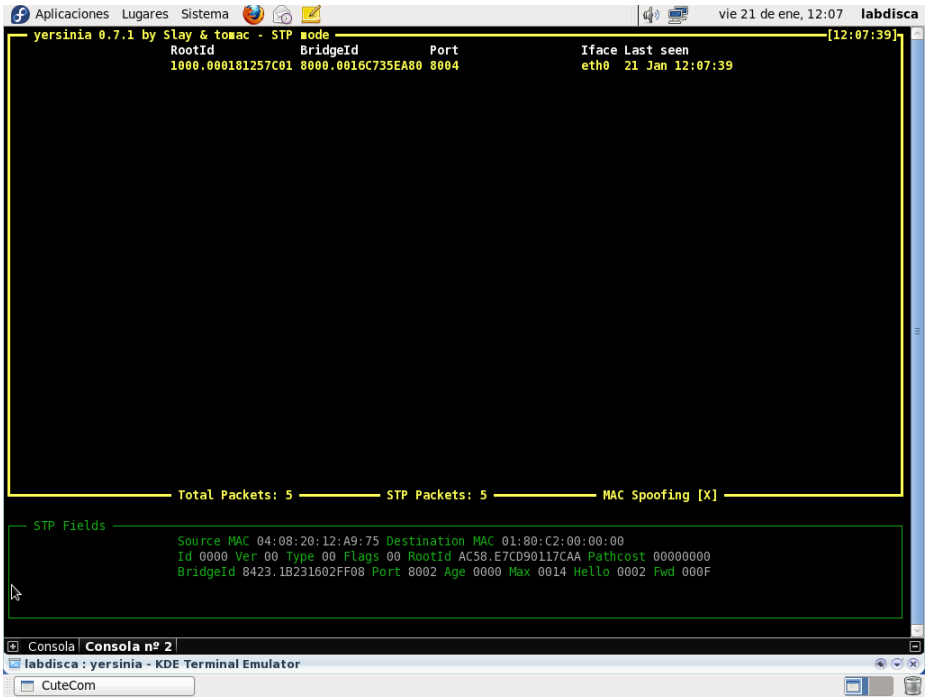


Figura 4.34: Paso 5: DHCP Starvation: Iniciando yersinia

Paso 6: Selecionamos la NIC que deseemos usar presionando i por defecto el toma la

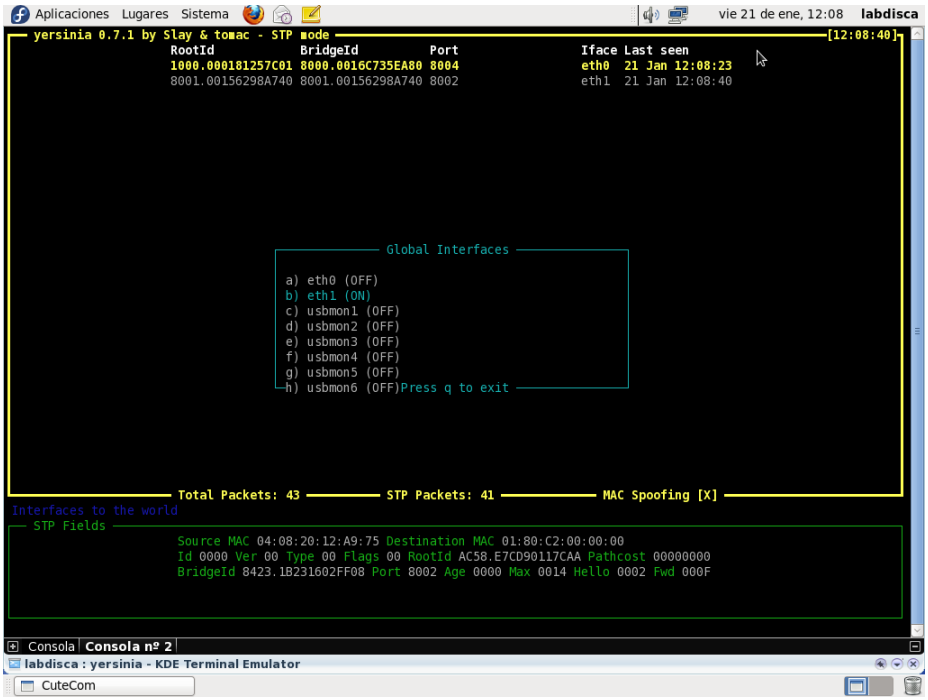


Figura 4.35: Paso 6: DHCP Starvation: Seleccionamos el puerto

primera interface que es eth0 presionamos la letra que corresponda a la NIC en este

caso la “a” para deselecionarla y selecionamos eth1 presionando la tecla “b” para selecionarla y luego presionamos la tecla “q” para salir. (Figura 4.35)

Nota: Cabe anotar que en yersinia los puertos no tienen el mismo nombre que en las terminales reales por eso eth0 y eth1 corresponden alos puertos eth2 y eth3 respectivamente.

Figura 4.36: Paso 7: DHCP Starvation: Seleccionando el tipo de ataque DHCP

Paso 7: Luego presionamos la tecla “g” para cargar el ataque, seleccionamos DHCP con “flecha arriba/abajo”. Y presionamos ENTER para seleccionar. (Figura 4.36)

Paso 8: Presionamos “x” para abrir el menu de ataques. Figura 4.37
Paso 9: Presionamos 1 para iniciar nuestro ataque.

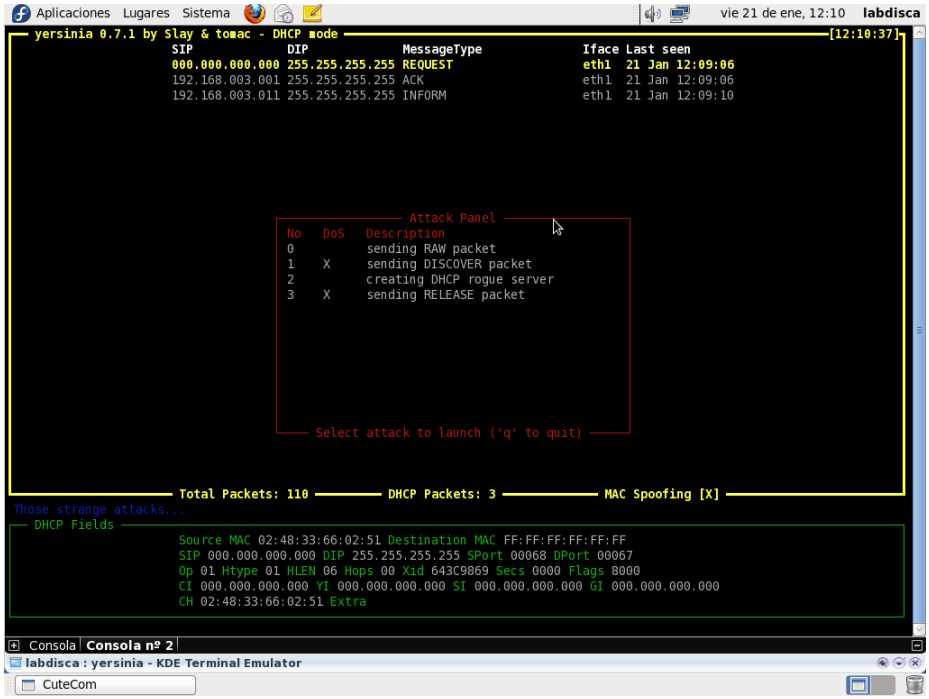


Figura 4.37: Paso 8: DHCP Starvation: Menú de ataques

Aqui ya hemos ejecutado nuestro ataque DHCP starvation.

4.6. Practica 6: Mitigación de DHCP Starvation.

Desde CUTECOM para evitar este ataque vamos a usar DHCP snooping.

Paso 10: Borramos la información del switch consultar "Anexos. Borrar la información de un Switch o Router Cisco."

Paso 11: Abrimos cutecom desde yakuake como root y accedemos al switch. Digitamos los siguientes comandos:

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch#hostname ALS1

ALS1(config)#ip dhcp snooping

ALS1(config)#ip arp inspection vlan 1

% Incomplete command.

ALS1(config)#

ALS1(config)#interface fa 0/2

ALS1(config-if)#

ALS1(config-if)#ip dhcp snooping trust

ALS1(config-if)#

ALS1(config-if)#ip arp inspection trust

ALS1(config-if)#

ALS1(config-if)#end

ALS1#

Hasta aquí ya hemos mitigado el ataque DHCP Starvation y nuestro switch comienza a filtrar mensajes de los puertos no confiables.

4.7. Práctica 7: Ataque DHCP Rouge.

4.7.1. Descripción.

Configurando un Servidor DHCP rogue es una de las técnicas en las que un atacante puede usar para ganar acceso al trafico de red. Este es alcanzado por respuestas spoofing que pueden ser enviadas por un Servidor DHCP autorizado.

4.7.2. Escenario.

El mismo que en DHCP Starvation.
Paso 1: Para este ataque continuamos desde el paso 5 del ataque DHCP starvatión

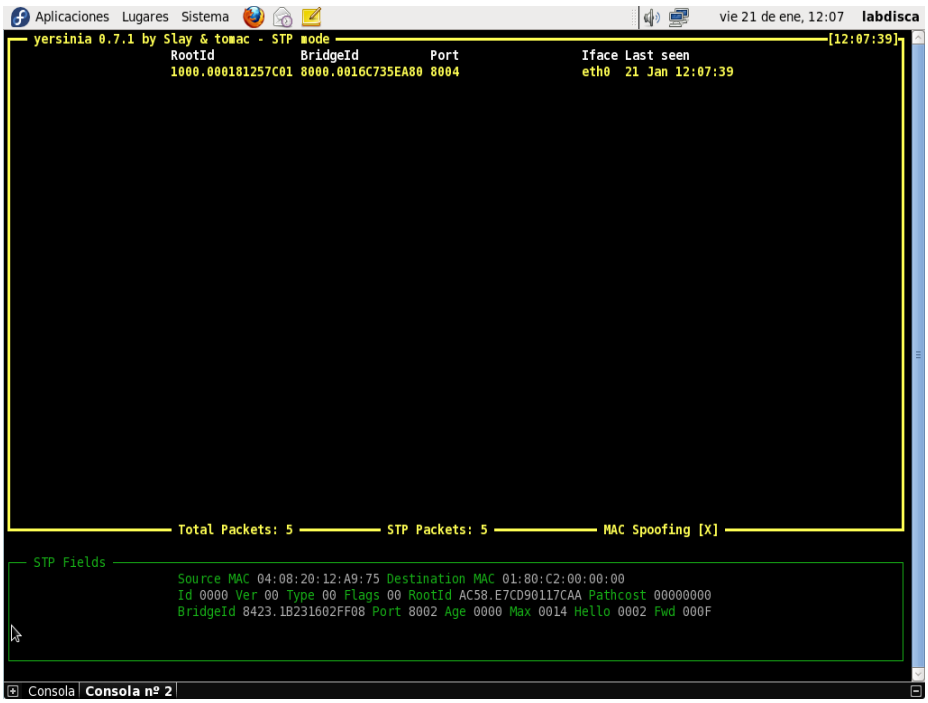


Figura 4.38: Paso 5: DHCP Rouge Server:Iniciando yersinia

Accedemos al Switch y borramos el Vlan.dat y el startup-config

4.7.3. DHCP Rouge Con Yersinia

Paso 5: Ejecutamos yersinia con digitando el comando yersinia -I.
Paso 6: Selecionamos la NIC que deseemos usar presionando i por defecto el toma la primera interface que es eth0 presionamos la letra que corresponda a la NIC en este

caso la “a” para deselecionarla y selecionamos eth1 presionando la tecla “b” para selecionarla y luego presionamos la tecla “q” para salir. (Figura 4.39)

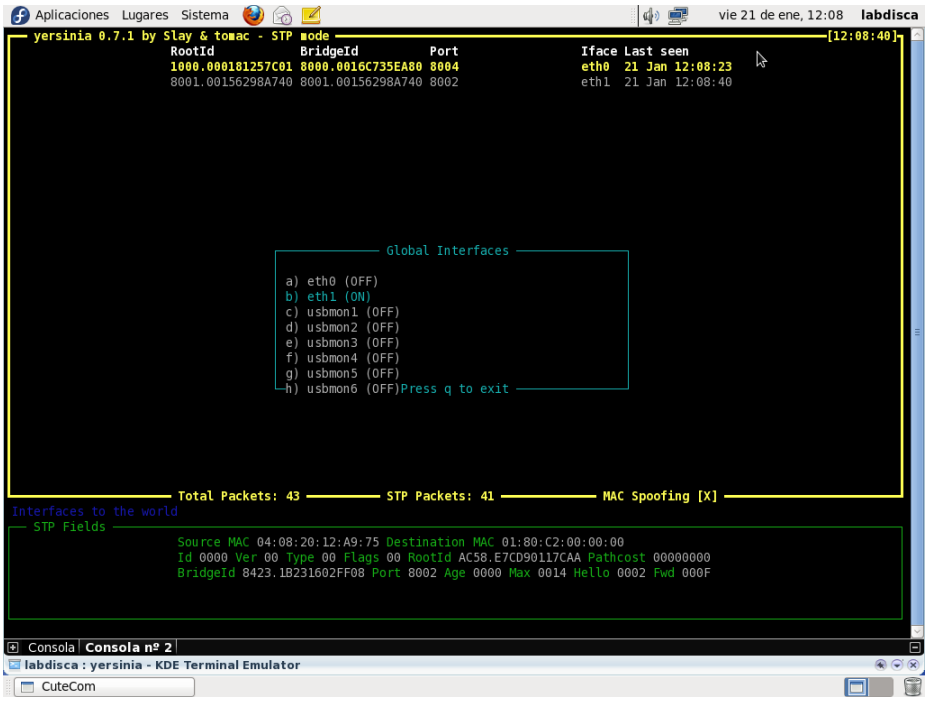


Figura 4.39: Paso 6: DHCP Rouge Server:Seleccionamos el puerto correspondiente

Nota: Cabe anotar que en yersinia los puertos no tienen el mismo nombre que en las terminales reales por eso eth0 y eth1 corresponden alos puertos eth2 y eth3 respectivamente.

Paso 7: Luego presinamos la tecla “g” para cargar el ataque, seleccionamos DHCP con “flecha arriba/abajo”. Y presionamos ENTER para seleccionar. (Figura 4.40)

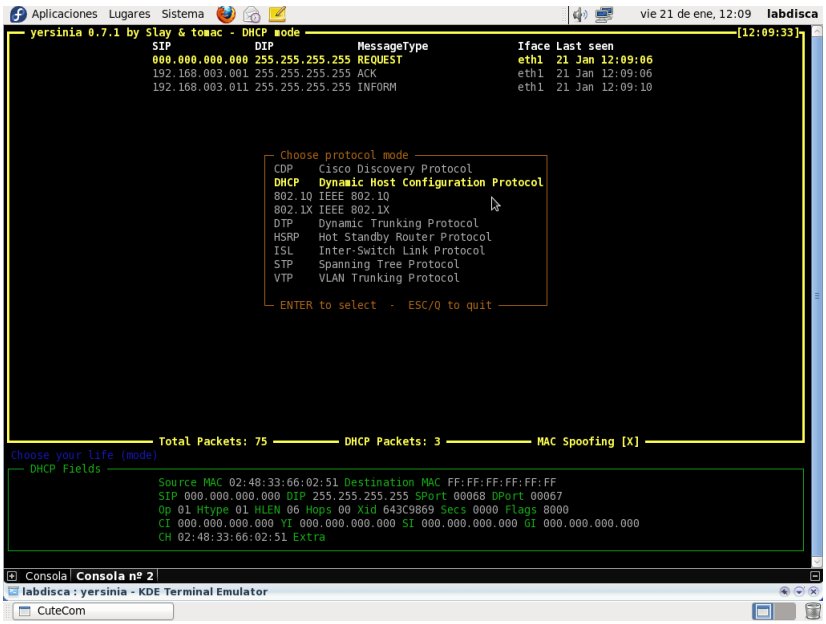


Figura 4.40: Paso 7: DHCP Rouge Server:Seleccionando el tipo de ataque DHCP

Paso 8: Presionamos “x” para abrir el menu de ataques. Figura 4.41

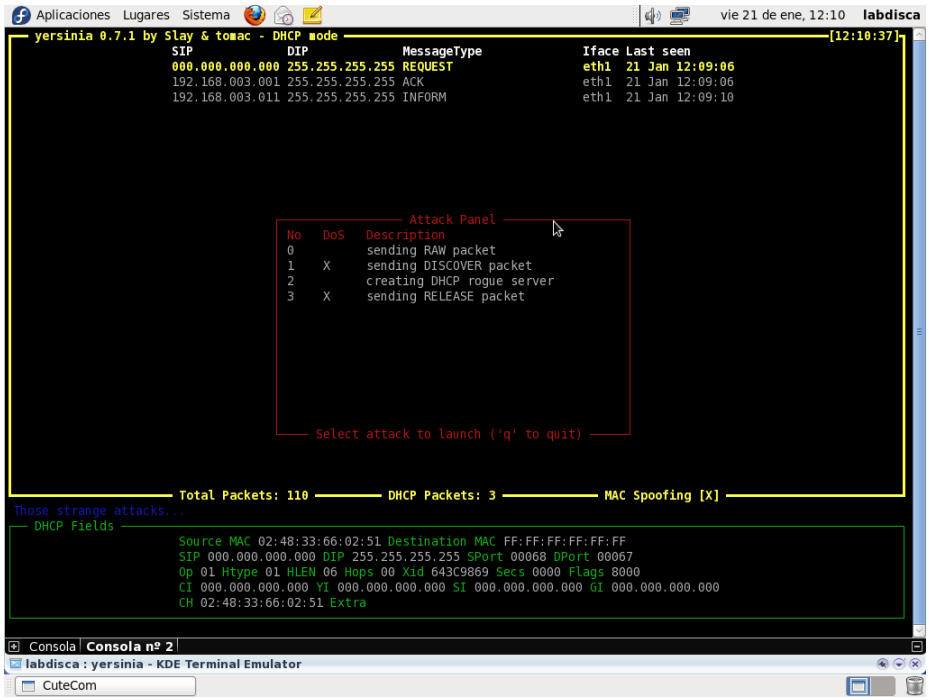


Figura 4.41: Paso 8: DHCP Rouge Server: Menú de ataques

Paso 9: Presionamos 2 para crear el servidor DHCP Rogue. (Figura 4.41)

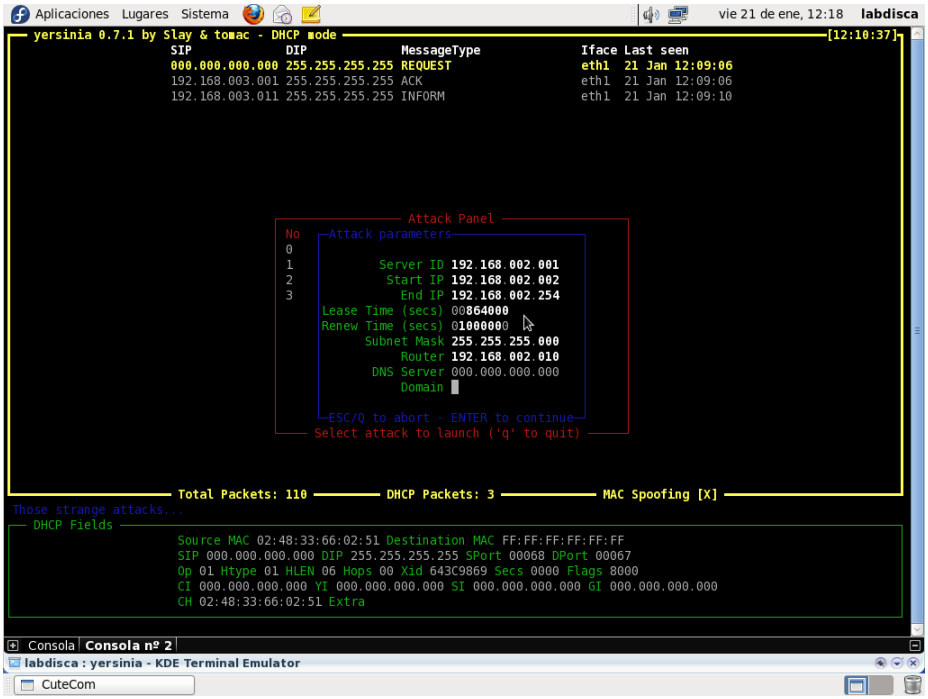


Figura 4.42: Paso 10: DHCP Rouge Server:Creando el Servidor DHCP rouge

Paso 10: Creamos servidor DHCP: Introducimos los parámetros de configuración del servidor. (Figura 4.42)

Nota: Es importante el servidor DHCP rouge se encuentre en la misma red de la Vlan que

vamos a atacar.

4.8. Practica 8: Mitigación de DHCP Rouge.

Desde CUTECOM para evitar este ataque vamos a usar DHCP snooping.

Paso 11: Borramos la información del switch consultar “Anexos. Borrar la información de un Switch o Router Cisco.”

Paso 12: Abrimos cutecom desde yakuake como root y accedemos al switch. Digitamos los siguientes comandos:

ALS1#config t

Enter configuration commands, one per line. End with CNTL/Z.

ALS1(config)#ip dhcp snooping

ALS1(config)#ip dhcp snooping vlan 1

ALS1(config)#interface fa0/2

ALS1(config-if)#ip dhcp snooping trust

ALS1(config-if)#ip dhcp snooping limit rate 2

ALS1(config-if)#end

4.9. Practica 9: Ataque Spanning Tree.

4.9.1. Escenario: Ataque STP Face 1

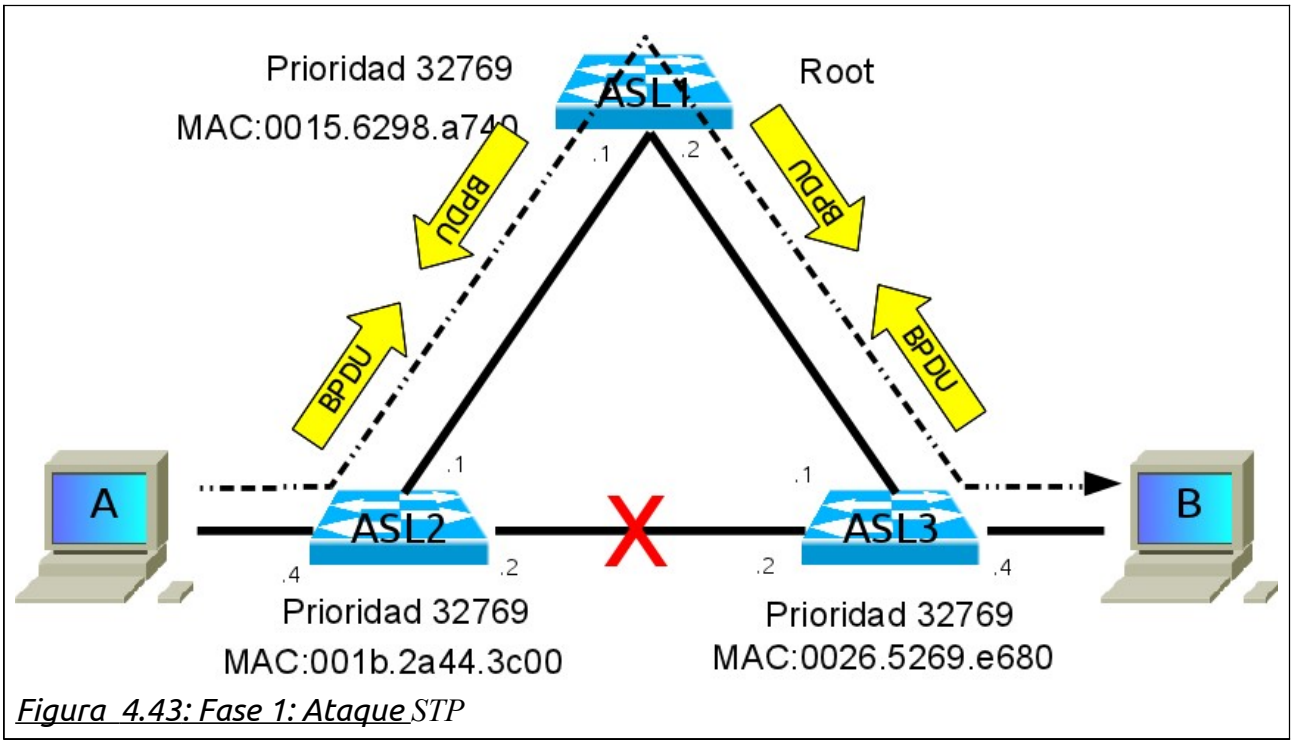


Figura 4.43: Fase 1: Ataque STP

Para este ataque haremos el montaje mostrado en el diagrama.

- Necesitamos tres Switches Cisco 2950 o 3650 catalyst.
- 2 Host
- Un Host con 2 targetas de red el cual va actuar como atacante.

Vamos a nombrar a los Switches ALS1, ALS2 y ALS3.

Paso 1: Borramos la información del switch consultar "Anexos. Borrar la información de un Switch o Router Cisco."

Paso 2: Ingresamos a Cutecom y configuramos cada uno de los Switches (Configuración inicial)

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#HOSTNAME ALS1

ALS1(config)#

ALS1(config)#end

ALS1#

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#HOSTNAME ALS2

ALS2(config)#

ALS2(config)#END

ALS2#

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#HOSTNAME ALS3

ALS3(config)#

ALS3(config)#END

ALS3#

Paso 3: Observamos como queda configurado el STP den cada uno de los switches.
ALS1>show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID   Priority   32769

Address   0015.6298.a740

This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0015.6298.a740
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

Vemos que el Switch ALS1 quedo como Root

Observamos como queda configurado el STPde ALS2...

```
ALS2>show spanning-tree

VLAN0001
 Spanning tree enabled protocol ieee
 Root ID    Priority    32769
        Address     0015.6298.a740
        Cost        19
        Port        1 (FastEthernet0/1)
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
        Address     001b.2a44.3c00
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------

Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
```

Observamos como queda configurado el STP. De ALS3..

ALS3>show spanning-tree

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0015.6298.a740
Cost 19
Port 2 (FastEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0026.5269.e680
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
---------- ---- --- --------- -------- --------------------------------
Fa0/1 Root FWD 19 128.2 P2p
Fa0/2 Altn BLK 19 128.3 P2p
Fa0/4 Desg FWD 19 128.5 P2p

4.9.2. Implementando Un Ataque STP Con Yersinia.

Paso 4: Ingresamos a Yakuake como root e ingresamos el comando:

[root@labdisca04 ~]# Yersinia -I (Figura 4.44)

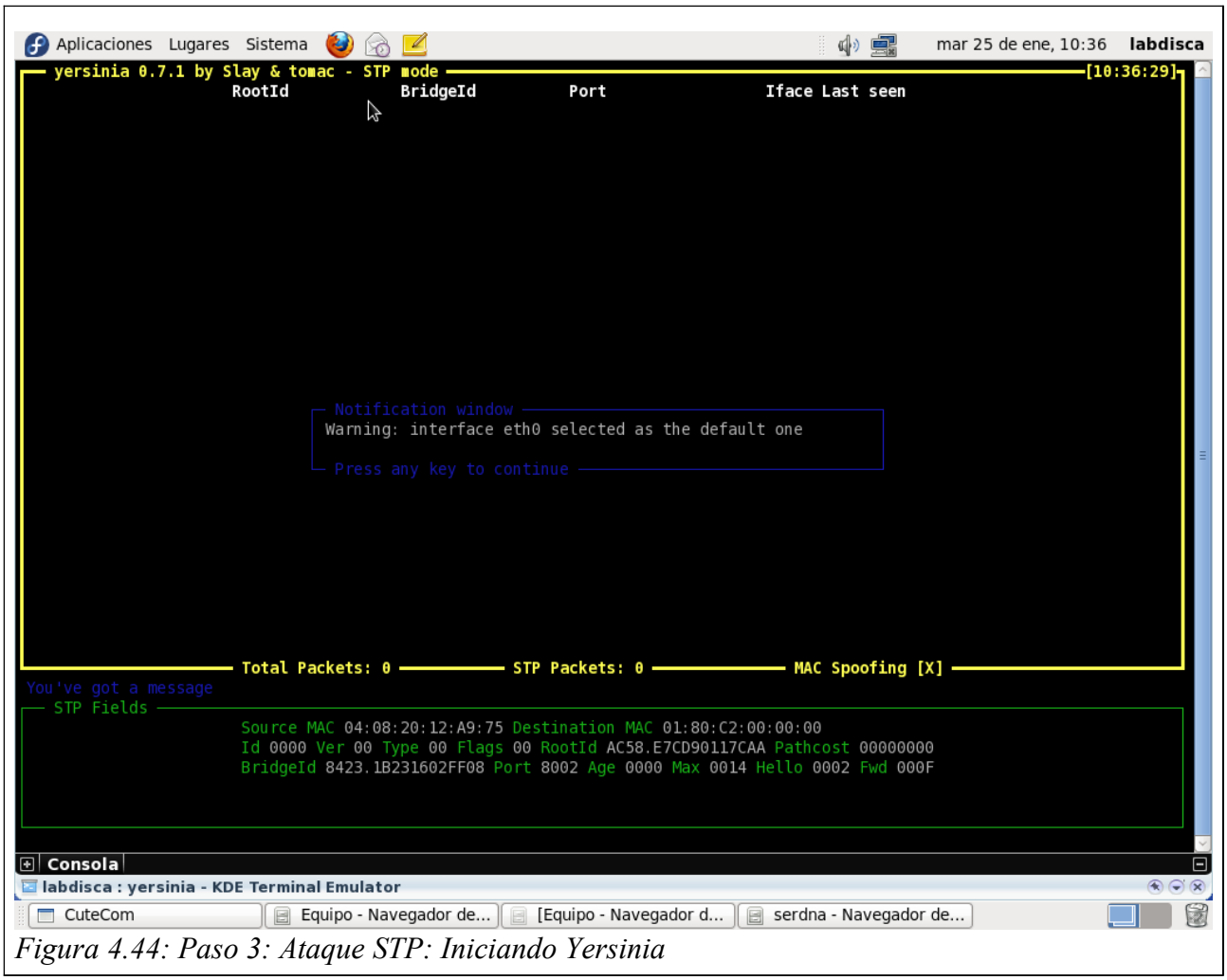


Figura 4.44: Paso 3: Ataque STP: Iniciando Yersinia

Paso 5: Digitamos i en el teclado y elegimos tanto eth0 como eth 1, estos corresponden a los puertos eth2 y eth3 de nuestro atacante pulsamos solamente b para elegir eth1 ya que eth0 esta por defecto. (figura 4.45)

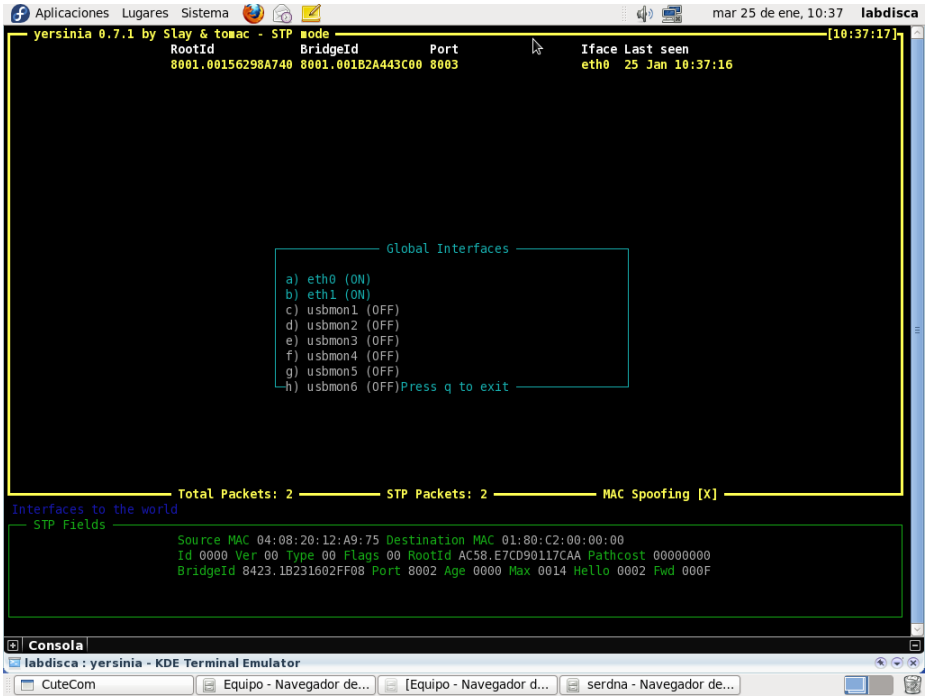


Figura 4.45: Paso 5: Ataque STP Eligiendo Puertos

Paso 6: Movemos Flecha arriba/ abajo y escogemos STP Spanning tree Protocol.

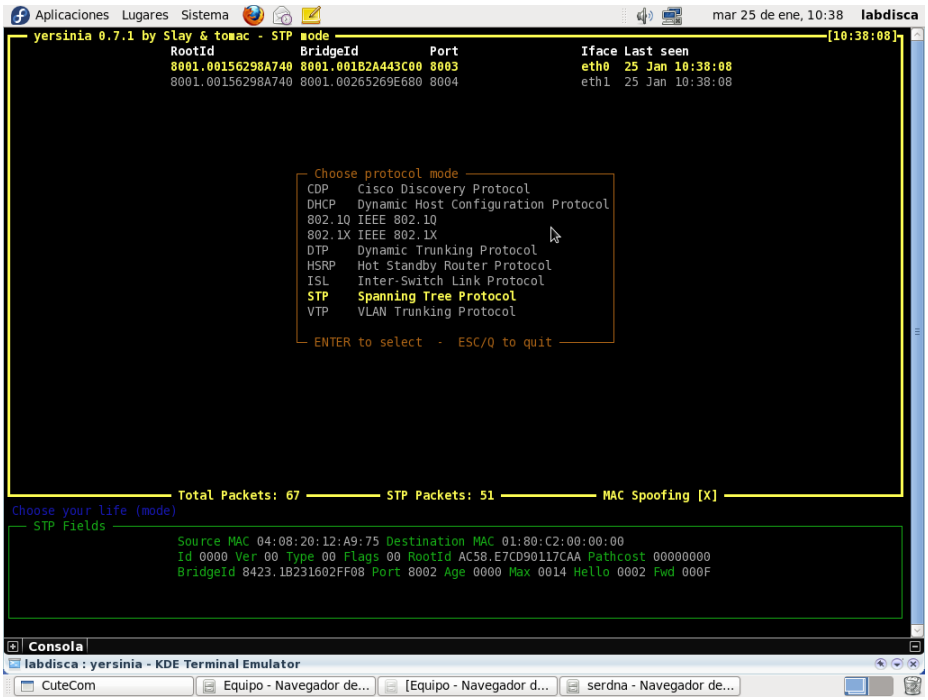


Figura 4.46: Paso 6: Ataque STP: Eligiendo tipo de ataque

Paso 7: Tecleamos x para entrar al menú de ataques y elegimos la opción 6 pulsando 6 en el teclado. Para convertirmos en Root

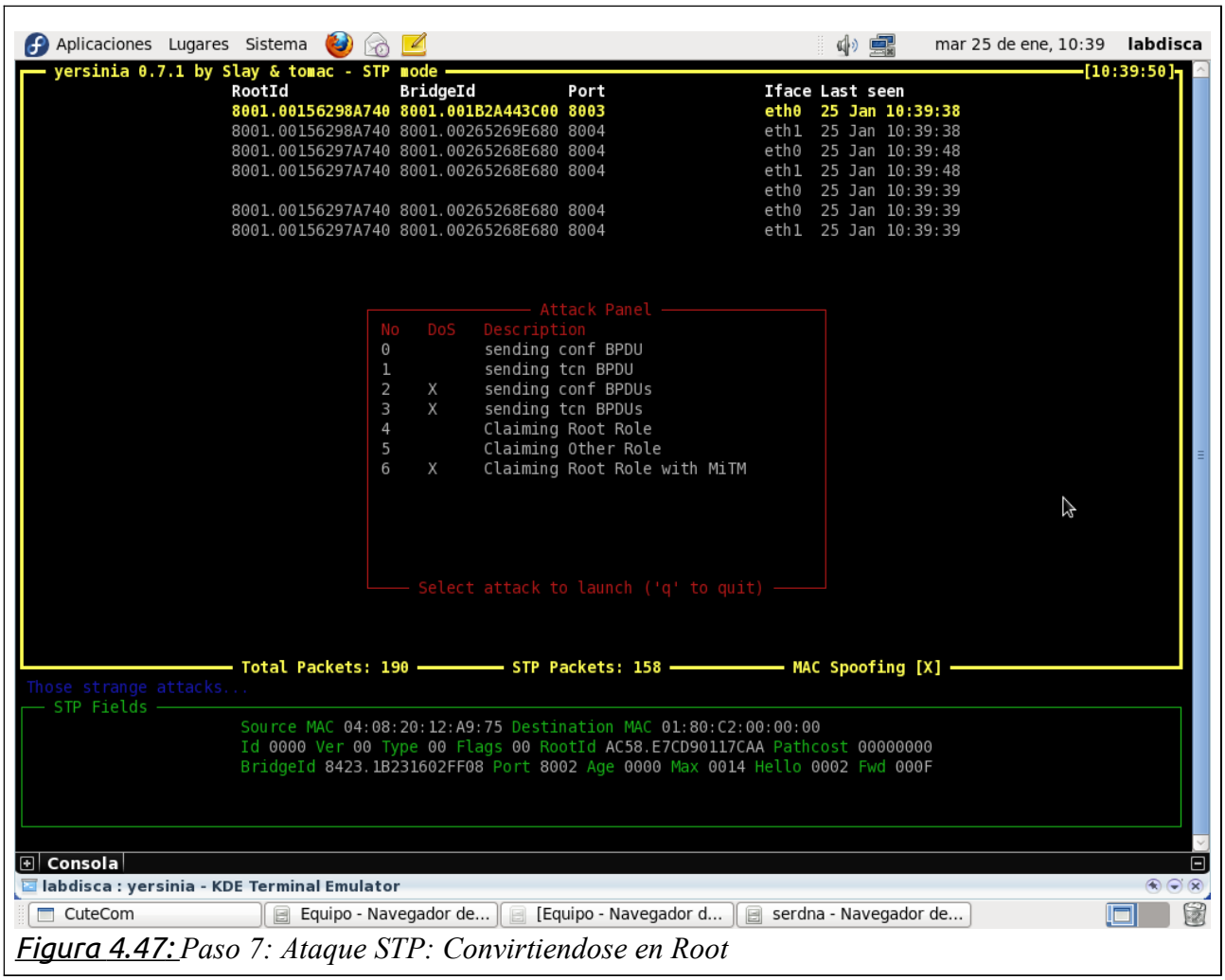


Figura 4.47: Paso 7: Ataque STP: Convirtiendose en Root

Paso 8: Ahora ingresamos a cutecom y verificamos nuevamente nuestro Spaning tree.

ALS1>show spanning-tree

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0015.6296.a740
Cost 57
Port 1 (FastEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0015.6298.a740
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p

ALS2>show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0015.6296.a740
             Cost        38
             Port        3 (FastEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     001b.2a44.3c00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------

Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

ALS3>show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0015.6296.a740
             Cost        38
             Port        4 (FastEthernet0/3)
```

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0026.5269.e680
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	*Role*	*Sts*	*Cost*	*Prio.Nbr*	*Type*
Fa0/1	*Desg*	*FWD*	*19*	*128.2*	*P2p*
Fa0/2	*Altn*	*BLK*	*19*	*128.3*	*P2p*
Fa0/3	*Root*	*FWD*	*19*	*128.4*	*P2p*
Fa0/4	*Desg*	*FWD*	*19*	*128.5*	*P2p*

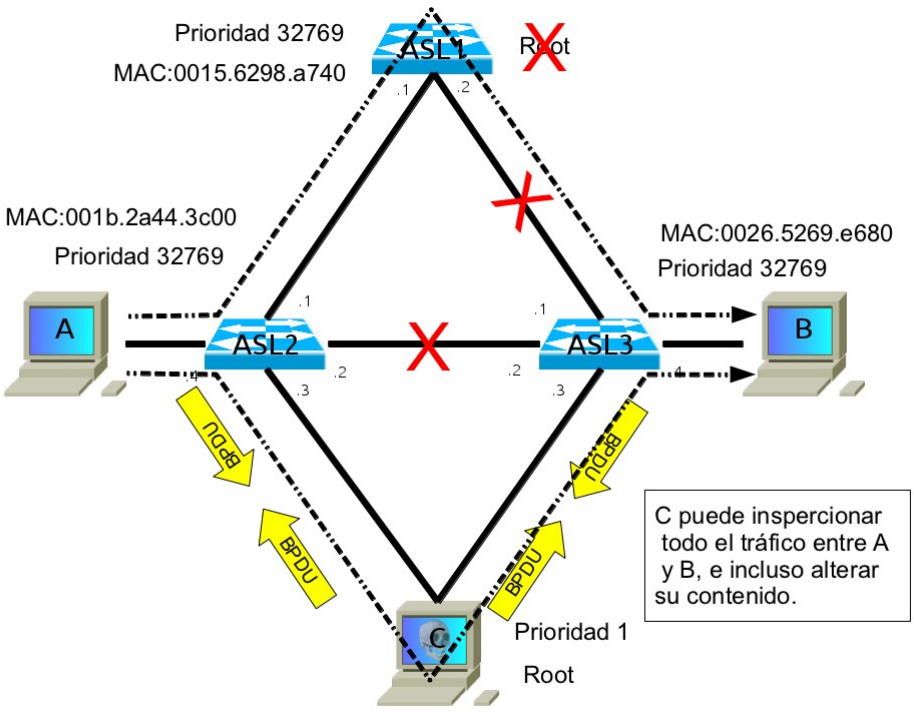


Figura 4.48: Fase 2: Ataque STP: Configuración STP despues del ataque

Si nos damos cuenta la configuración del STP ha cambiado. Y el ALS1 dejo de ser root la configuración nueva se muestra en el gráfico (Figura 4.48)

4.10. Practica 10: Mitigación Ataque STP: Root Guard

Para mitigar el ataque STP vamos a usaremos BPDU Guard en cada uno de los los puertos donde esten conectados nuestros host.

Paso 9: Ingresamos a cutecom y configuramos ALS2 y ALS3 con RootGuard. Que es donde tenempos conectados nuestras terminales.

ALS2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ALS2(config)#interface range fastEthernet 0/3 - 4
ALS2(config-if-range)#spanning-tree guard root
ALS2(config-if-range)#end
ALS2#

ALS3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ALS3(config)#interface range fastEthernet 0/3 - 4
ALS3(config-if-range)#spanning-tree guard root
ALS3(config-if-range)#end
ALS3#

En un campo real es recomendable configurar Root guard en todos los puertos que no esten conectados a otros switches.

Paso 9: verificamos nuevamente el Spanning-Tree en cada uno de los Switches.

LS1>show spanning-tree

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0015.6298.a740
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0015.6298.a740
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/1 Desg FWD 19 128.1 P2p

Fa0/2 Desg FWD 19 128.2 P2p

Vemos que el Switch ALS1 quedo como Root

Observamos como queda configurado el STPde ALS2...

ALS2>show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0015.6298.a740

Cost 19

Port 1 (FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 001b.2a44.3c00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/1 Root FWD 19 128.1 P2p

Fa0/2 Desg FWD 19 128.2 P2p

Fa0/4 Desg FWD 19 128.4 P2p

Observamos como queda configurado el STP. De ALS3..

ALS3>show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0015.6298.a740

Cost 19

Port 2 (FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0026.5269.e680

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/1 Root FWD 19 128.2 P2p

Fa0/2 Altn BLK 19 128.3 P2p

Fa0/4 Desg FWD 19 128.5 P2p

Obeservamos que vuleve a estar el Switch ALS1 como root.

ANEXOS

A. Configuracion de una ip estática en Fedora

Paso 1: En la parte superior derecha (figura 1) hacemos click derecho en el icono de conexiones de red.

Figura 1: "Conexiones de red"

Paso 2: Se nos abre una ventana (figura 2) de conexiones de red. En esta ventana selecionamos la interfaz a configurar.

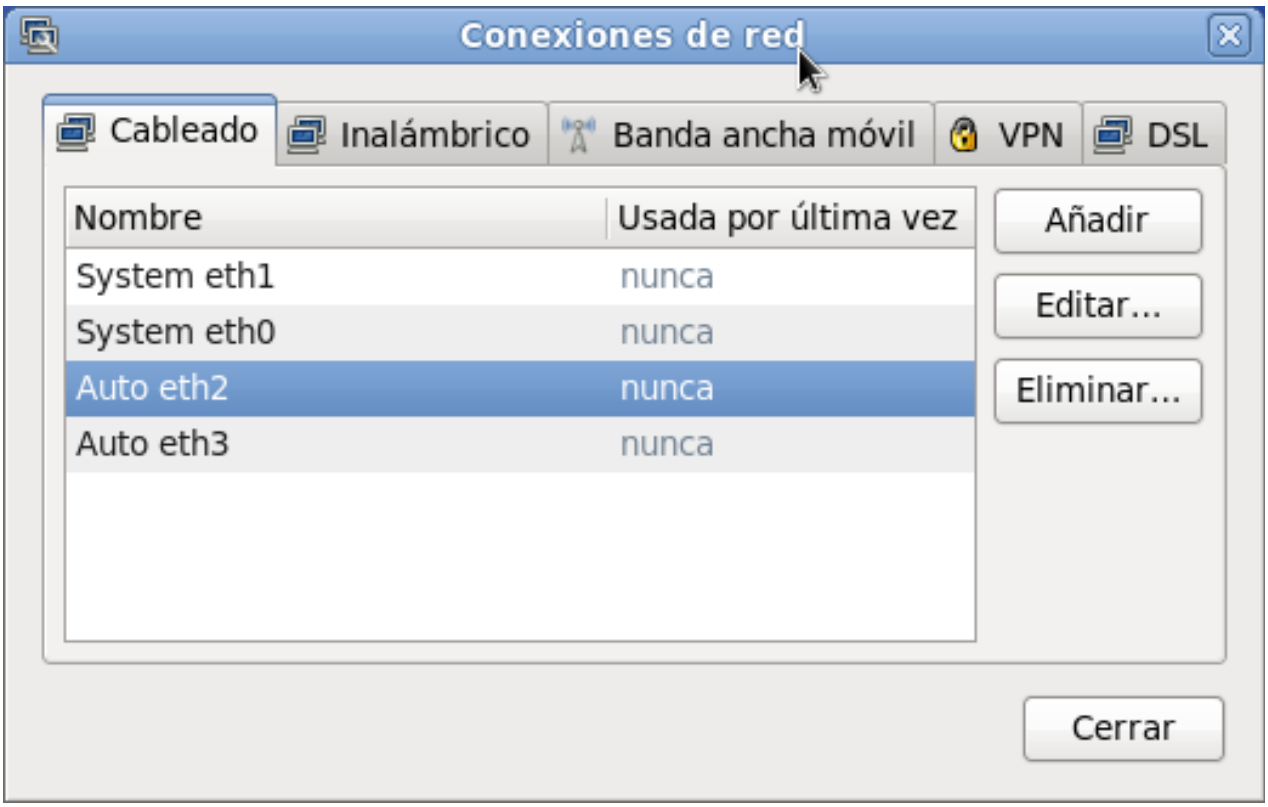


Figura 2: Conexiones de red: Eligiendo terminal

Paso 3: Nos pide autenticarnos para poder editar la interfaz selecionada, esta será pedida en el momento que vayamos a guardar la configuración. A continuación hacemos click en editar (figura 3).

Paso 4: Se abre la ventada Editando Auto (Interfaz) nos aseguramos que el método este en manual (si la colocamo en automática el servidor DHCP le asignaria automáticamente la dirección, esto siempre y cuando haya un servidor DHCP en la

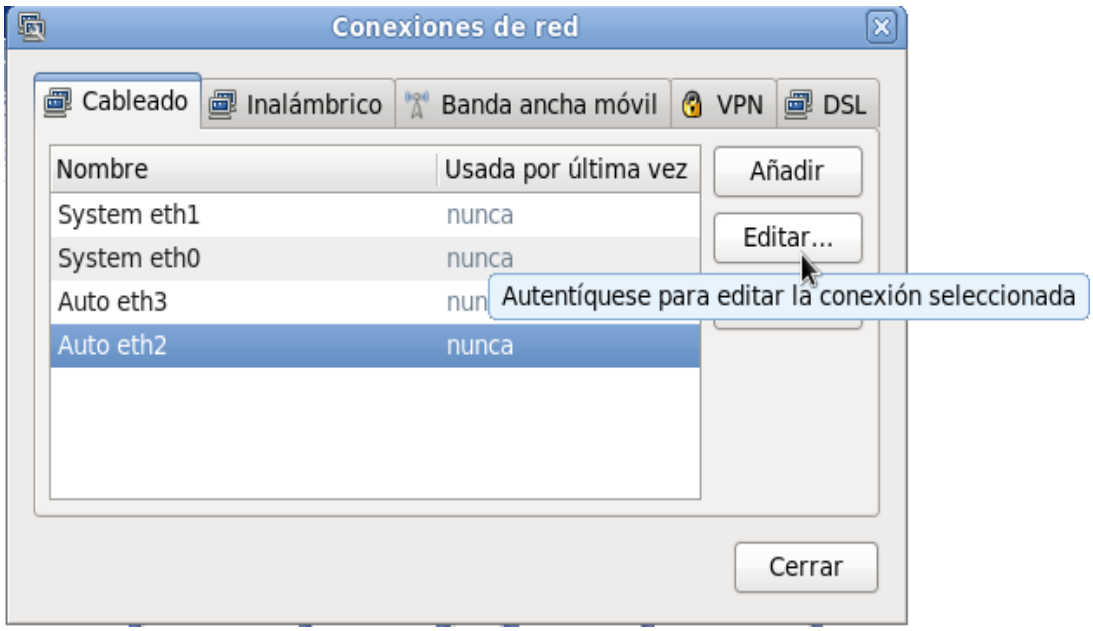


Figura 3: Mensaje antes de editar

red) y luego hacemos click en añadir e ingresmos: la IP, la mascara en número para el ejemplo mostrado (figura 4) sería 24 que corresponde a la máscara 255.255.255.0 y por último la puerta de enlace que sería la ip de la Vlan a la que pertenece el equipo o si estamos conectados a un router sería el "default gateway[23]"

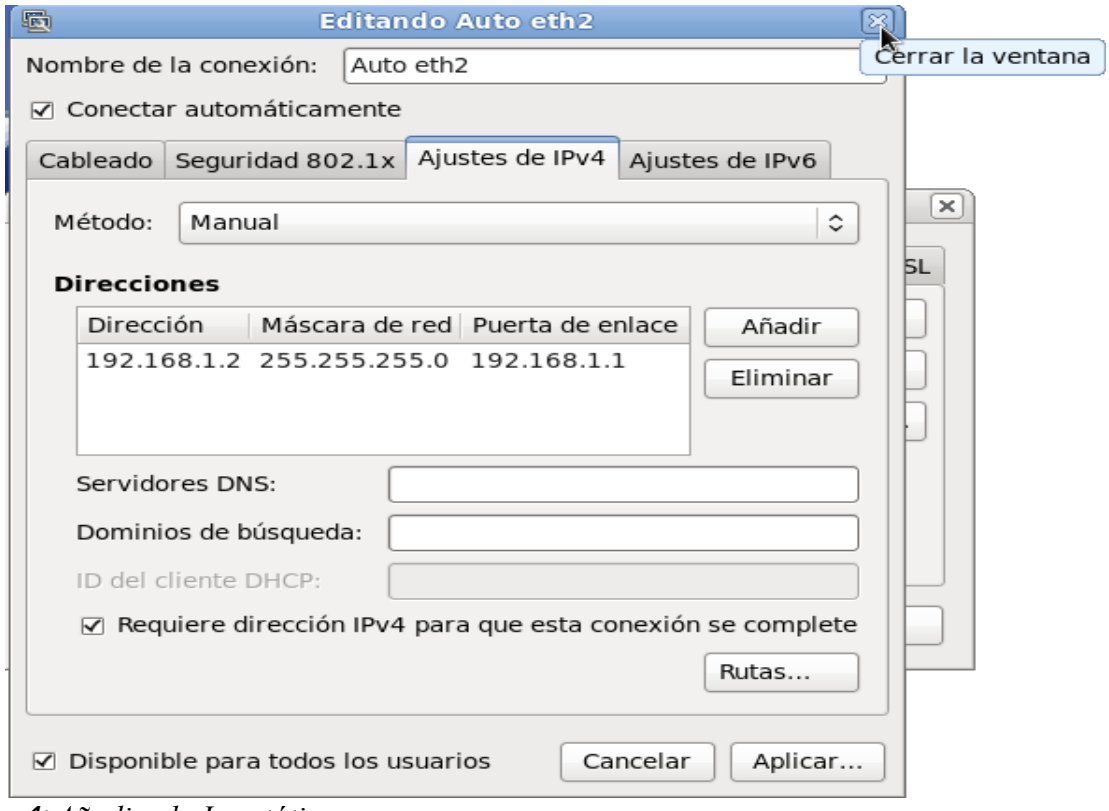


Figura 4: Añadiendo Ip estática

Paso 4: Hacemos click en aplicar nos pedira la contraseña del administrador, y

23 ***Puerta de enlace*** *en español.*

obtenemos nuestra dirección IP estática.

B. Limpiando la configuración del Router/ Switch

Borramos el archivo vlan.dat...

Switch#delete vlan.dat[24]
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#

Eliminamos la configuración de inicio...

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#

hacemos la recarga en el switch...

Switch#reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]
1d20h: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
Base ethernet MAC Address: 00:0a:b8:a9:d7:80
Xmodem file system is available.
The password-recovery mechanism is enabled.
Initializing Flash...
flashfs[0]: 349 files, 5 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 15998976
flashfs[0]: Bytes used: 7909888
flashfs[0]: Bytes available: 8089088
flashfs[0]: flashfs fsck took 9 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs) installed, fsid: 3
done.

---

24 *Es una base de datos que guarda la configuración del VTP (VLAN trunking Protocol)*

Loading "flash:c3560-ipservices-mz.122-25.SEB4/c3560-ipservices-mz.122-

*25.SEB4.bin"...@@
@@@@@@@@@@@@@@@@@@@@@@@@*

*@@
@@*

*@@
@@*

*@@
@@*

*@@
@@*

CONCLUSIONES

- Hasta este punto se tiene la capacidad para distinguir los ataques básicos que se pueden presentar a nivel de capa 2 y como prevenirlos
- Se tiene la capacidad de mejorar la seguridad en la red, de acuerdo a su configuración y montaje.
- Se tiene la capacidad de manejar diferentes herramientas de ataque y como emplearlas
- Se tiene la capacidad de emplear diferentes herramientas de Seguridad Dispositivos Cisco de acuerdo a su montaje en la red.

GLOSARIO

3

3com: 3Com NASDAQ: COMS es uno de los líderes en fabricación de equipos para infraestructura de Redes Informáticas. El nombre 3Com hace referencia a que los intereses de la compañía son Computadoras, Comunicaciones y Compatibilidad.
http://es.wikipedia.org/wiki/3Com

A

Ad-hoc: En redes de comunicación, una red ad hoc es aquella (especialmente inalámbrica) en la que no hay un nodo central, sino que todos los dispositivos están en igualdad de condiciones. Ad hoc es el modo más sencillo para el armado de una red. Sólo se necesita contar con 2 placas o tarjetas de red inalámbricas (de la misma tecnología).
http://es.wikipedia.org/wiki/Ad-hoc
Algoritmo: En matemáticas, ciencias de la computación y disciplinas relacionadas, un algoritmo (del latín, dixit algorithmus y éste a su vez del matemático persa Al Juarismi) es un conjunto preescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien lo ejecute. Dados un estado inicial y una entrada, siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución. *http://es.wikipedia.org/wiki/Algoritmo*
ARP: *Address Resolution protocol* http://es.wikipedia.org/wiki/Address_Resolution_Protocol

B

BPDU: Bridge Protocol Data Units (BPDUs) son frames que contienen información del protocolo Spanning tree (STP). Los switches mandan BPDUs usando una única dirección MAC de su puerto como mac de origen y una dirección de multicast como MAC de destino (01:80:C2:00:00:00) .
BPDU Guard: (*PortFast Bridge Protocol Data Unit (BPDU) guard*), esta característica del protocolo Spanning Tree es una mejora que CISCO crea. Mejora la fiabilidad, manejabilidad y seguridad del Switch.
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a008009482f.shtml

C

CAM: *Content Addressable Memory* http://en.wikipedia.org/wiki/CAM_Table
Canales: El trunking es una función para conectar dos switchs, routers o servidores, del mismo modelo o no, mediante 2 cables en paralelo en modo Full-Duplex. Así se consigue un ancho de banda del doble para la comunicación entre los switches. Esto permite evitar cuellos de botella en la conexión de varios segmentos y servidores. El protocolo es 802.1ad.
http://es.wikipedia.org/wiki/Trunking_%28red%29

Capa De Enlace De Datos: El nivel de enlace de datos (en inglés data link level) o capa de enlace de datos es la segunda capa del modelo OSI, el cual es responsable de la transferencia fiable de información a través de un circuito de transmisión de datos. Recibe peticiones de la capa de red y utiliza los servicios de la capa física.
http://es.wikipedia.org/wiki/Nivel_de_enlace_de_datos
CISCO: Cisco Systems es una empresa multinacional con sede en San Jose (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones. *http://es.wikipedia.org/wiki/Cisco*
Conmutador: Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. *http://es.wikipedia.org/wiki/Switch*

D

Denial-of-service: En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés *Denial of Service)*, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. *http://es.wikipedia.org/wiki/Ataques_de_denegaci%C3%B3n_de_servicio*
DOS Attack: *Denial of service attack*. Es un intento de hacer un recurso de la computadora no está disponible para sus usuarios *http://en.wikipedia.org/wiki/Denial-of-service_attack*
DSniff: Es un paquete de utilidades que incluye código para analizar muchos protocolos de aplicación diferentes y extraer información interesante http://en.wikipedia.org/wiki/DSniff, http://www.itillious.com/insight/articles/dsniff.html
DTP: (Dynamic Trunking Protocol) es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

E

Enrutador: El enrutador (calco del inglés router), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. *http://es.wikipedia.org/wiki/Enrutador*
Ettercap: Ettercap es un interceptor/sniffer/registrador para LANs con switch, existente para la mayoría de las plataformas.Una vez que empieza a rastrear el tráfico, obtendrás un listado de todas las conexiones activas, junto a una serie de atributos acerca de su estado (active, idle, killed, etc.). El asterisco indica que una contraseña fue recogida en esa conexión. *http://ettercap.sourceforge.net/forum/viewtopic.php?t=2329*

F

FreeNAC: FreeNAC proporciona asignación virtual LAN, LAN de control de acceso (para

todo tipo de dispositivos de red tales como servidores, estaciones de trabajo, impresoras, teléfonos IP ..), detección de terminales live network. *http://freenac.net/*

G

GARP: *Gratuitous ARP o ARP announcement Gratuitous* en este caso significa una petición / respuesta que normalmente no es necesario de acuerdo a la especificación de ARP (RFC 826), pero podría ser utilizado en algunos casos. *Una solicitud ARP request en un paquete ARP request donde la fuente y destino IP son colocados conjuntamente a la IP de la maquina que expide el paquete y la destinación MAC que es la direcci{on Broadcast ff:ff:ff:ff:ff:ff. Regularmente, no debe ocurrir ningun paquete Reply. Un GARP reply es una respuesta a la cula no hay ninguna solicitud hecha.* http://wiki.wireshark.org/Gratuitous_ARP

H

Hijacking: significa "secuestro" en inglés y en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñarse o robar algo (generalmente información) por parte de un atacante. *http://es.wikipedia.org/wiki/Hijacking*

HUB: tambien conocido como concentrador. Es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. *http://es.wikipedia.org/wiki/Concentrador*

HTTP: Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web.
http://es.wikipedia.org/wiki/HTTP

HTTPS: Hyper Text Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hiper Texto, es decir, es la versión segura de HTTP.
http://es.wikipedia.org/wiki/HTTP

I

ICMP: *Internet Control Message Protocol* **.** Es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado. *http://es.wikipedia.org/wiki/ICMP*

IEEE 802.1Q: *El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.*
http://es.wikipedia.org/wiki/IEEE_802.1Q

ISL: es un protocolo propietario de Cisco que mantiene información sobre VLANs en el tráfico entre routers y switches.
http://es.wikipedia.org/wiki/ISL

L

LAN: Una red de área local, red local o LAN (del inglés *local area network*) es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc.
http://es.wikipedia.org/wiki/LAN
Lrzsz: Es un paquete estéticamente modificado zmodem / YMODEM / xmodem construido a partir de la versión de dominio público del paquete de Chuck Forsberg rzsz.
http://packages.debian.org/stable/comm/lrzsz

M

MAC: *E*n redes de ordenadores la dirección MAC (*siglas en inglés de Media Access Control o control de acceso al medio*) es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una ethernet de red.
http://es.wikipedia.org/wiki/MAC_address
Macof. Herramienta usada para crear ataques MAC.
http://seclists.org/bugtraq/1999/May/55 (*Enlace del código fuente*).
MITM: *Man in the middle.* Es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado *http://es.wikipedia.org/wiki/Ataque_Man-in-the-middle*
Modelo OSI: El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. *http://es.wikipedia.org/wiki/Modelo_OSI*

N

Nivel De Red: El nivel de red o capa de red, según la normalización OSI, es un nivel o capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones.

P

Ping: es una utilidad diagnóstica en redes de computadoras que comprueba el estado de la conexión del host local con uno o varios equipos remotos por medio de el envío de paquetes ICMP de solicitud y de respuesta. *http://es.wikipedia.org/wiki/Ping*
PKI: Es un framework que Provee un mecanismo para manejar claves criptográficas. El uso de este framework es limitado por redes de infraestructura fijada.
Pradip Lamsal - Helsinki University of Technology-Telecommunications Software and Multimedia Laboratory.
Pong: Pong (o *Tele-Pong*) fue un videojuego de la primera generación de videoconsolas publicado por Atari, creado por Nolan Bushnell y lanzado el 29 de noviembre de 1972. *http://es.wikipedia.org/wiki/Pong*
Puerto: Un puerto de red es una interfaz para comunicarse con un programa a través de una red. Un puerto suele estar numerado. La implementación del protocolo en el destino utilizará ese número para decidir a qué programa entregará los datos recibidos. Esta asignación de puertos permite a una máquina establecer simultáneamente diversas conexiones con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes.
http://es.wikipedia.org/wiki/Puerto_de_red
Puerto Trunk: Es aquel que tiene acceso a todas las VLANs.

R

RARP: *Reverse Adress resolution Protocol.* Protocolo usado para resolver la IP de una dirección de Hardware dada.
http://es.wikipedia.org/wiki/RARP

RFC: – *Request for comments.* Petición por comentarios. Documentos que se iniciaron en 1967 que describen los protocolos de internet.
http://es.wikipedia.org/wiki/Request_For_Comments

Root Guard: Es una característica del protocolo STP. Esta característica mejora lña confiabilidad, manejabilidad y seguridad de la red conmutada.
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800ae96b.shtml

S

Span Path Cost: Parametro configurable del spanning Tree para el el camino de menor coste.
http://es.wikipedia.org/wiki/Spanning_tree (Funcionamiento I).
Spoofing. en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación

http://es.wikipedia.org/wiki/IP_spoofing
Sniffer: programa de captura de las tramas de red.
http://es.wikipedia.org/wiki/Packet_sniffer
SSL: Secure Sockets Layer (SSL; protocolo de capa de conexión segura) y su sucesor Transport Layer Security (TLS; seguridad de la capa de transporte) son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.
SSH: *Secure Shell* Interprete de ordenes segura en español sirve para acceder a las máquinas remotas a través de una red.
http://es.wikipedia.org/wiki/Secure_Shell
STP: *Spanning Tree Protocol (SmmTPr)* es un protocolo de red de nivel 2 de la capa OSI, (nivel de enlace de datos). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones) *http://es.wikipedia.org/wiki/Spanning_tree*
Switch Port Stealing: *Se utiliza en casos donde no podemos usar un envenenamiento ARP, por el tema de las tablas estáticas.*
http://coffeeattack.blogspot.com/2007_09_01_archive.html
SYN_cookies: Mecanismo de proteccion contra Inundación SYN,
http://es.wikipedia.org/wiki/SYN_cookies

T

TCP/IP: es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. *http://es.wikipedia.org/wiki/TCP/IP*
Trunking: Canales en español.

U

UDP: permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera, *http://es.wikipedia.org/wiki/User_Datagram_Protocol*

V

VLAN: una VLAN (acrónimo de *Virtual LAN*, 'Red de Área Local Virtual') es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del Dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3 y 4). *http://es.wikipedia.org/wiki/VLAN*
VLAN Hopping: Las VLANs también pueden servir para restringir el acceso a recursos de red con independencia de la topología física de ésta, si bien la robustez de este método es discutible al ser el salto de VLAN (VLAN hopping) un método común de evitar tales medidas de seguridad. *Referencia VLAN*
VLT: El etiquetado VLT (sigla para *Virtual LAN Trunk*) es un sistema 3Com que permite a un

puerto ser colocado en todas las VLANs definidas por su switch. *http://listas.ubiobio.cl/pipermail/admin-redes/attachments/20071018/a6caa03a/attachment-0001.doc*

VMPS: es un conmutador de red que contiene un mapeo de la información del dispositivo a la VLAN. *http://en.wikipedia.org/wiki/VLAN_Management_Policy_Server*

Y

Yersinia: Framework usado para ataques en capa 2 *http://www.yersinia.net/*

C. LINKS EXTERNOS

- *http://www.elgaragevirtual.com.ar/2009/07/ataques-basados-en-la-mac-y-el.html*
- *http://www.gabriel-arellano.com.ar/*
- *http://www.tech-faq.com/es/vlan-hopping.html*
- http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml#wp39211 *Double-Encapsulated 802.1Q/Nested VLAN Attack*