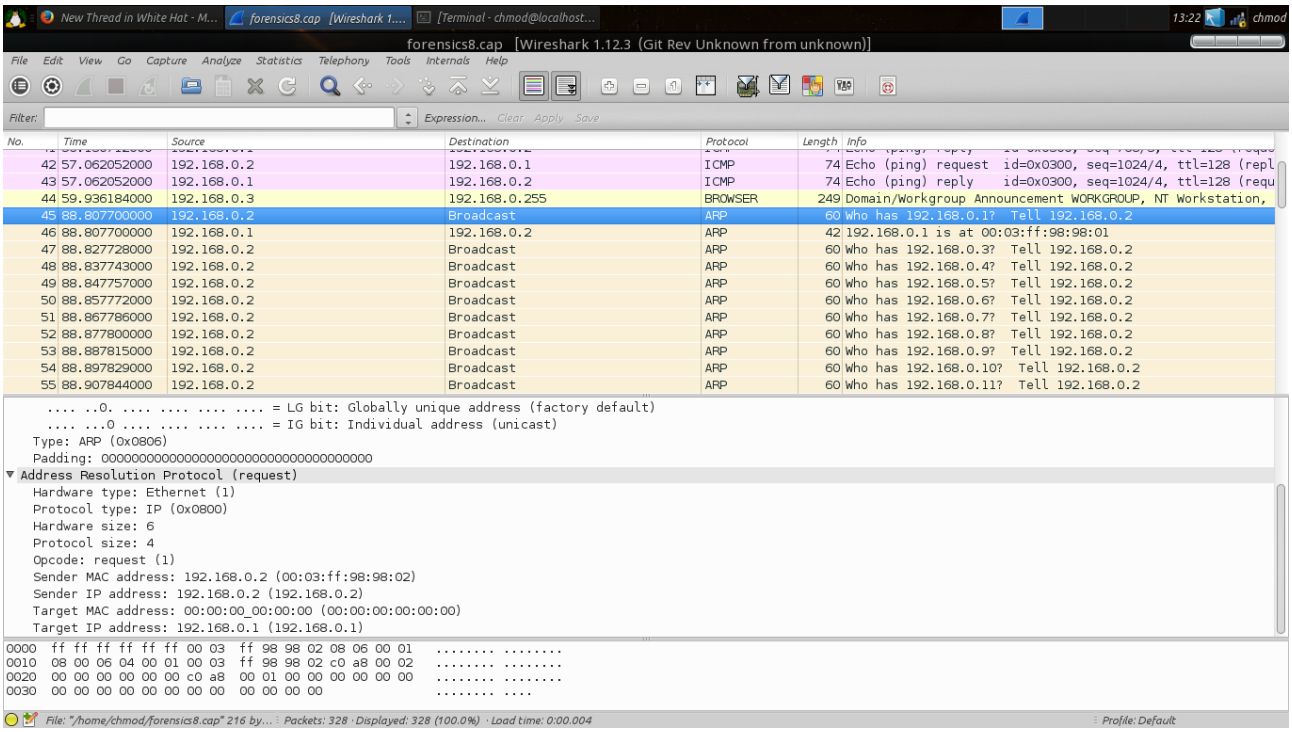
Trabajo análisis de protocolos



Alumno Ignacio Rojas
Profesor Miguel Varas
Curso 292 - B
Fecha: 28/12/2015

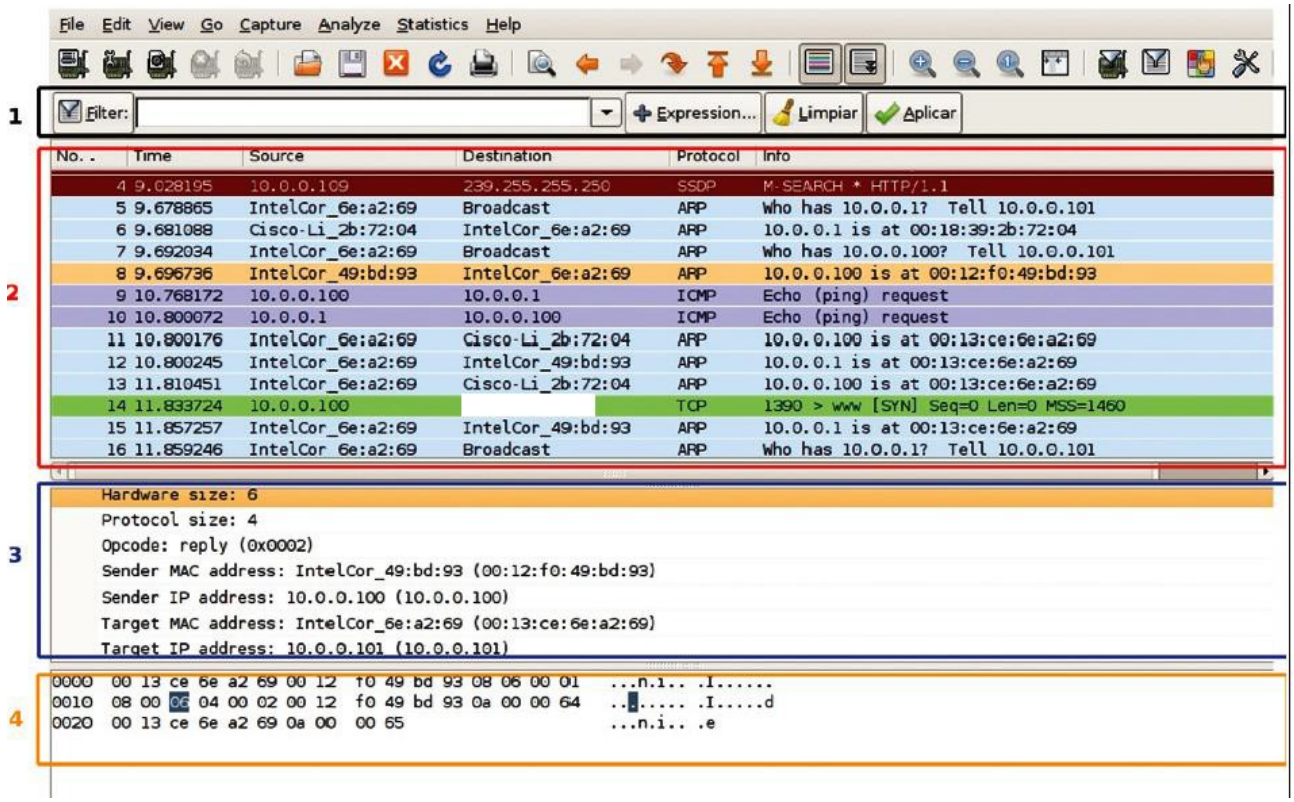
Introducción

Muchas veces en los ordenadores de una empresa la red esta congestionada. Las causas de estos problemas puede ser por una mala configuración de la red como por ej: tormentas broadcast, spanning-tree mal configurado, enlaces redundantes, etc. Pero, también, puede tratarse de ataques realizados por terceros que pretenden dejar fuera de servicio un servidor web mediante un ataque DoS, husmear tráfico mediante un envenenamiento ARP o simplemente infectar los equipos con código malicioso para que formen parte de una red zombi o botnet.

El trabajo está dividido en dos ataques simulados llevados a cabo en la red de área local, estos son: ARP Spoof, DHCP Spoof. Para detectar los ataques DoS se emplea Wireshark como herramienta principal.También, se proponen acciones de mitigación para los dos casos expuestos.

¿Porque se usa wireshark?

Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente; y todo ello por medio de una interfaz sencilla que permite desglosar por capas cada uno de los paquetes capturados proporcionando así al administrador de redes información necesaria para abordar tareas en el análisis de trafico.



A continuación, describo las 4 zonas indicadas en la figura:

* La zona 1 es el área de definición de filtros y, como veremos más adelante, permite definir patrones de búsqueda para visualizar aquellos paquetes o protocolos que nos interesen.

* La zona 2 se corresponde con la lista de visualización de todos los paquetes que se están capturando en tiempo real.

* La zona 3 permite desglosar por capas cada una de las cabeceras de los paquetes seleccionados en la zona 2.

* La zona 4 representa, en formato hexadecimal, el paquete en bruto, es decir, tal y como fue capturado por nuestra tarjeta de red.

Snifer – Descripcion de resultados

Cada entrada del resultado del análisis contiene la siguiente información: criticidad, grupo, protocolo y resumen. Los diferentes niveles usados son los siguientes, entre paréntesis se informa del color utilizado en el GUI:

Chat (gris): información sobre flujos normales. Se trata de información normal que ayuda a entender qué ha ocurrido como, por ejemplo, un segmento TCP con el flag SYN.

Nota (cian): situaciones destacables fuera del funcionamiento normal. Por ejemplo, que una aplicación devuelva un código de error común como HTTP 404.

Advertencia (amarillo): indica atención. Se debe prestar especial cuidado a los paquetes marcados de esta forma ya que puede tratarse de intentos de ataque como, por ejemplo, que una aplicación devuelva un código de error inusual como un problema de conexión.

Error (rojo): problemas graves como paquetes mal formados.

Los tipos de grupo que nos podemos encontrar son los siguientes:
Checksum: una suma de comprobación no es válida.

Secuencia: secuencias de protocolo sospechosas como, por ejemplo, que el número de secuencia no es continuo o se ha detectado una retransmisión.

Código de Respuesta: problemas con códigos de respuesta de aplicaciones, por ejemplo, la respuesta "HTTP 404 Página no encontrada".

Código de petición: una petición a un aplicación. Por ejemplo, "File Handle == x)". Normalmente se mostrará con criticidad de Chat.

Sin decodificar: disección incompleta o los datos no se pueden decodificar por otros motivos.

Ensamblado: problemas en el reensamblado. Por ejemplo, no se cuenta con todos los fragmentos u ocurrió una excepción durante el proceso.

Protocolo: violación de las especificaciones del protocolo como, por ejemplo, los valores de campo son inválidos o las longitudes ilegales.

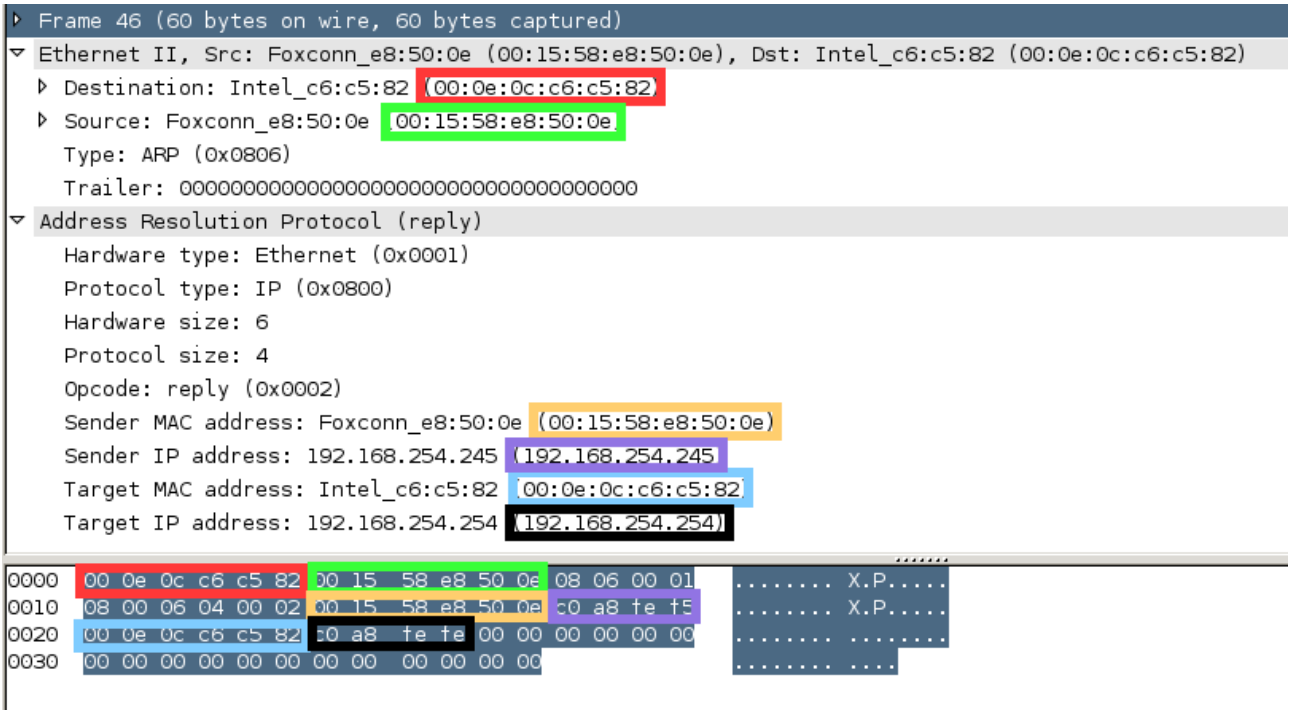
Mal formados: paquetes mal formados o en el análisis se produjo un error que produjo que se abortara el análisis.

Protocolo Arp – ataque DoS Arp Spoof

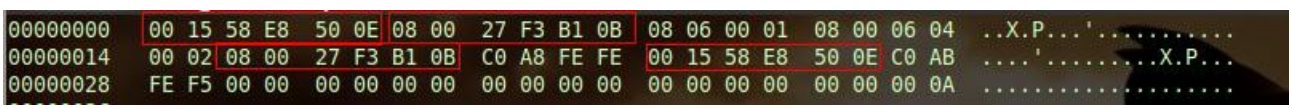
El Arp Spoof es utilizado por atacantes para interponerse entre una o varias máquinas con el fin de interceptar, modificar o capturar paquetes. Esta técnica, se ve reflejada en la Figura 5- Áreas de Wireshark donde se puede observar que algo sospechoso está ocurriendo debido a la gran cantidad de tráfico ARP que se está recibiendo. Si observamos más detalladamente el comportamiento del protocolo, nos daremos cuenta de que el servidor está siendo víctima de un ataque DoS.

En el paquete número 5 (De la imagen arriba) se puede ver cómo la máquina con IP 10.0.0.101, con una MAC IntelCor_6e:a2:69, ha lanzado un ARP request a la dirección broadcast preguntando por la MAC de la IP 10.0.0.1 (el gateway de nuestra red). Acto seguido, el router contesta con un ARP reply indicando cuál es su dirección MAC. A continuación, la misma IP repite el proceso y pregunta por la MAC de la IP 10.0.0.100 (servidor de ficheros) mediante otra difusión broadcast. El servidor contesta con su dirección MAC (IntelCor_49: bd:93). Hasta aquí todo normal. Tenemos una máquina de nuestra LAN (10.0.0.101), que ya tiene la MAC del servidor y la del router con las cuales ya puede compartir tráfico Ethernet. El problema viene a partir del paquete 11, donde la máquina anterior envía reiteradamente a nuestro server y al router paquetes ARP reply falsos, asociando la IP de ambos con su propia MAC (IntelCor_6e:a2:69). De esta forma, todo el tráfico que transite entre el gateway de la LAN y el server pasará a través de la máquina atacante.

A continuación, se muestra el formato en bruto de una respuesta ARP generada por nuestro equipo a un ARP request. Podemos buscar estos paquetes con el siguiente filtro arp.opcode == 0x0002 (ARP reply):



Acto siguiente se clickea con el botón derecho el frame y se selecciona “Export Selected Packet Bytes” y se guarda la trama en el fichero. Luego con cualquier editor hexadecimal se modifica la trama creando un ARP reply. En la siguiente imagen se suplanta con el ip 192.168.254.245 con MAC 00:15:58:e8:50:0e haciendose pasar por el gateway (IP 192.168.254.254 con MAC 00:0e:0c:c6:c5:82):



Existen multitud de herramientas gratuitas destinadas a detectar este tipo de ataques (Arpwatch, Nast, Snort, Patriot NG, ArpON, etc) que permiten generar alertas cuando se detecta un uso anormal del protocolo ARP. Cuando se detecta cambios en las asignaciones ARP/IP significa un uso anormal del protocolo

```
root@Mordor:~# arpwatch -n 192.168.254.0/24 -i eth0
root@Mordor:~# tail -f /var/log/syslog | grep -i arpwatch
Oct 19 09:16:42 Mordor arpwatch: listening on eth0
Oct 19 09:16:56 Mordor arpwatch: flip flop 192.168.254.254 08:00:27:f3:b1:0b (00:0e:0c:c6:c5:82) eth0
Oct 19 09:16:56 Mordor arpwatch: flip flop 192.168.254.254 08:00:27:f3:b1:0b (00:0e:0c:c6:c5:82) eth0
Oct 19 09:17:02 Mordor arpwatch: flip flop 192.168.254.245 08:00:27:f3:b1:0b (00:15:58:e8:50:0e) eth0
Oct 19 09:17:02 Mordor arpwatch: flip flop 192.168.254.245 08:00:27:f3:b1:0b (00:15:58:e8:50:0e) eth0
Oct 19 09:17:07 Mordor arpwatch: ethernet mismatch 192.168.254.254 08:00:27:f3:b1:0b (00:0e:0c:c6:c5:82) eth0
```

.

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

Protocolo DHCP - DHCP SPOOF

Esta técnica consiste en falsificar paquetes DHCP. El ataque consiste en instalar un DHCP falso o un software que emule las funciones del mismo de tal forma que responda a peticiones DHCPDISCOVER de los clientes. Es necesario analizar los pasos llevados a cabo entre un cliente y un servidor DHCP legítimo

Cuando un equipo se conecta a la red y solicita una dirección IP envía un DHCPDISCOVER a la dirección broadcast (UDP) esperando respuesta por algún servidor DHCP.

Éste contestará a tal petición enviando un paquete unicast denominado DHCPOFFER y que contiene varios parámetros de configuración (IP, gateway, etc.).

Hasta este punto, el cliente puede recibir ofertas de varios servidores DHCP por lo que utilizará el siguiente criterio de elección: si la oferta propuesta se corresponde con una dirección previamente asignada (ya que son recordadas por el cliente), el cliente seleccionará ésta. En caso de que la propuesta no esté relacionada con una dirección IP previa, el cliente adquirirá la primera oferta recibida.

En respuesta a esta oferta, el cliente enviará un DHCPREQUEST a la dirección broadcast pidiendo autorización para utilizar esa configuración a lo que el servidor responderá, o bien con un paquete unicast DHCPACK autorizando el uso de dicha configuración, o bien con un DHCPNAK denegando el uso de tales parámetros.

El protocolo DHCP no proporciona mecanismos de autenticación que permitan verificar el origen de los paquetes durante la negociación de estos parámetros de configuración. Por lo tanto, nada impide que un atacante pueda falsificar paquetes DHCPOFFER proporcionando información falsa al cliente.

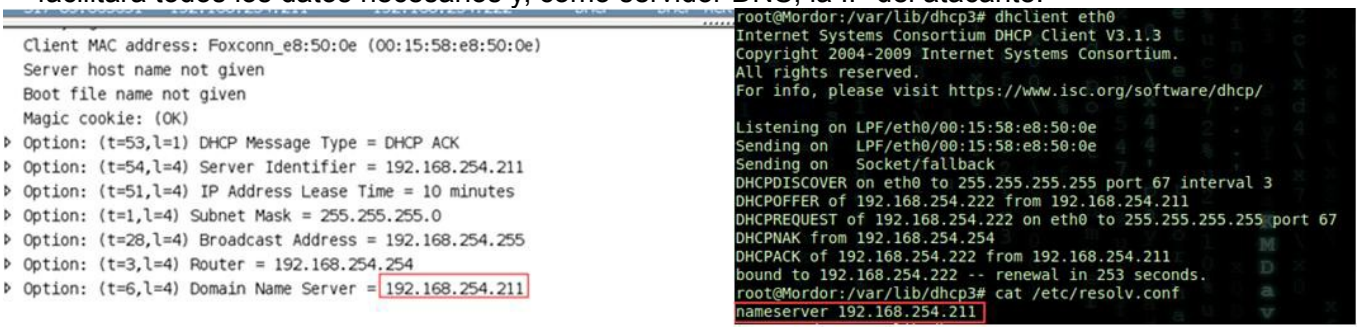
```
ddns-update-style none;

authoritative;

subnet 192.168.254.0 netmask 255.255.255.0 {
interface eth0;
range 192.168.254.222 192.168.254.225;
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.254.255;
option routers 192.168.254.254;
option domain-name-servers 192.168.254.211;
}
```

Por ejemplo: Un atacante configura un servidor dhcpd3 en su equipo Linux con los parámetros mostrados en la figura anterior (/etc/dhcp3/dhcpd.conf)

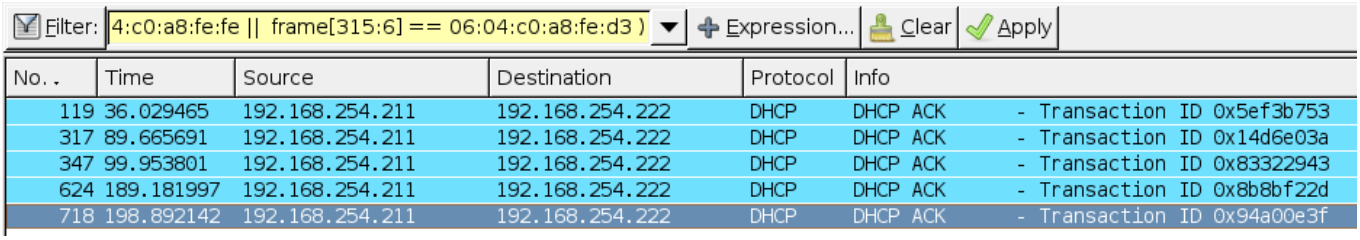
En él se configura un rango de 4 direcciones IP en desuso (que puede obtener entre aquellas que no tengan un registro DNS PTR, que no estén escuchando por servicios comunes o simplemente escuchando respuestas legítimas del servidor DHCP) y un default gateway legítimo (192.168.254.255), pero especifica como servidor DNS la IP del atacante (192.168.254.211). Además, prepara Ettercap para falsificar ciertas respuestas DNS:

echo www.inteco.es A 192.168.254.211 >> /usr/share/ettercap/etter.dns

Cuando un usuario se conecta a la red y solicita una IP por DHCP, nuestro servidor falso le facilitará todos los datos necesarios y, como servidor DNS, la IP del atacante:

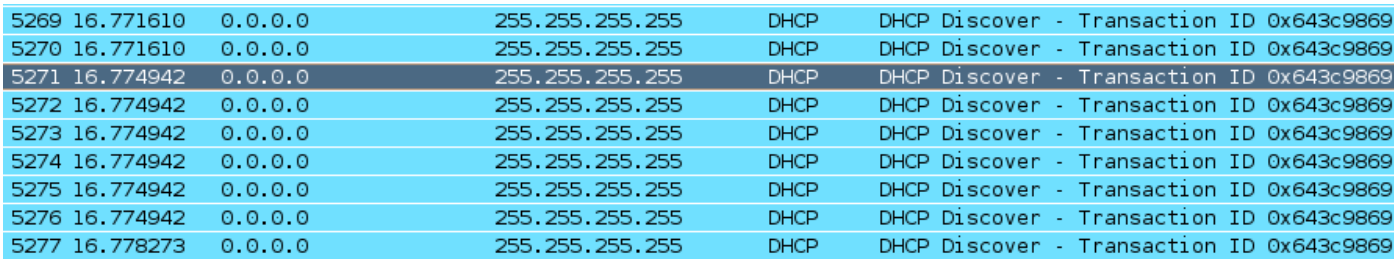


Además de las herramientas citadas anteriormente, para alertar sobre estas situaciones, podríamos hacer uso de filtros en Wireshark para acelerar la búsqueda de respuestas ACK con un DNS o un gateway diferentes al configurado en nuestro servidor DHCP: bootp.option.value == 05 && (frame[309:6] != 03:04:c0:a8:fe:fe || frame[315:6] == 06:04:c0:a8:fe:d3)



De esta manera, indicamos que muestre aquellas tramas enviadas por el servidor DHCP que no contengan la IP del gateway o un servidor DNS legítimo.

Otro tipo de ataque similar al flooding con paquetes ARP consiste en enviar multitud de paquetes DHCP DISCOVER utilizando MACs de origen aleatorias con el objetivo de acabar con el rango de direcciones IP disponibles en el servidor DHCP (DHCP Exhaustion). Detectar esta inundación (flooding) resulta más sencillo que en el caso anterior debido a la excesiva cantidad de paquetes DHCP DISCOVER enviados por segundo:



Una posible solución para estos problemas es configurar ACLs en el switch impidiendo que aquellos puertos de acceso destinados a equipos de usuario, envíen paquetes UDP cuyo puerto origen sea 67 para evitar de esta forma el uso de servidores DHCP no legítimos en nuestra red.

Conclusión

El wireshark es una herramienta muy util para detectar y acotar problemas en las redes. Es una herramienta simple de instalar, configurar y posee una interfaz intuitiva para usarla.

La seguridad de la red es muy importante para una empresa. En este caso se simulan ataques DoS y se proveen métodos para detectarlos con el sniffer y posteriormente repararlos. El sniffer wireshark es una herramienta muy optima para una empresa ya que un administrador puede detectar fácilmente problemas en la red.

La estructura del protocolo arp consta de cuatro direcciones, el hardware y la dirección de protocolo del remitente y el receptor host.

La estructura del protocolo dhcp es un protocolo cliente/servidor que consiste en una lista de direcciones ip dinamicas y se va asignando a los clientes en forma de “alquiler” sabiendo en que momento ese host tiene una ip determinado y por cuanto tiempo.