Estrategia de seguridad contra ataques internos en redes locales

***Andrés Subert Semanat*[1]**

[1]*Universidad de Oriente, Departamento de telecomunicaciones, asubert@fie.uo.edu.cu*

RESUMEN

A pesar de las topologías de seguridad de redes basadas en Cortafuegos, Enrutadores y Conmutadores es posible romper la seguridad interna de las redes y realizar ataques de suplantación de identidades de equipos y de usuarios. El envenenamiento de la tabla del Protocolo de Resolución de direcciones es uno de los ataque interno mas efectivos

En este trabajo se discuten y comparan tres topologías de red según las cuales se puede segmentar y aislar las vulnerabilidades encontradas en una red local, las variantes de solución demuestran ser efectivas en entornos académicos, donde la mayoría de las violaciones de seguridad provienen de empleados internos.

Palabras Clave: Seguridad en Redes

Security strategy against internal attacks in local area networks

ABSTRACT

In spite of network security topologies which are based on Firewalls, Routers and Switches, it is possible to break the internal security of the networks and to carry out user and terminal spoofing attacks. The poisoning of Address Resolution Protocol table is one of the more effective attacks that can be made from inside the network.

In this issue, three network topologies are discussed according to which it will be possible to segment and isolate those vulnerabilities that can be found in a local area network. The found solutions show to be effective in academic environments, where most of the security violations come from insiders.

Key Words: Network security

INTRODUCCIÓN

En los últimos tiempos, en las redes internas de Centros universitarios han ocurrido afectaciones a la seguridad del sistema, debido a esto surge la necesidad de realizar un estudio de las diferentes formas que emplean personas malintencionadas con el fin de sustraer información personal, suplantar identidades y poner en riesgo la seguridad de los servidores y de otros clientes. Por ejemplo, cuando tiene lugar el robo de contraseñas de acceso a los servidores de Internet, (donde existen unas políticas del uso de sus recursos), se visitan sitios que contienen información censurada, se puede poner en entredicho la confiabilidad y el prestigio del usuario y de la institución.

Los referidos ataques afectan a muchos usuarios y no se debe esperar a recibir ataques de más trascendencia para buscar soluciones al problema, pues si se tiene almacenada una información sensible, ésta debe ser protegida antes de que tales hechos ocurran y así evitar las consecuencias de la violación de las normas y mantener la confiabilidad de la red.

El ataque ético al sistema (el administrador ataca su propia red para conocer sus debilidades) aunque genera las dudas de la seguridad del mismo, facilita al administrador el conocimiento de las debilidades del sistema para poder garantizar el servicio de la manera más segura y confiable.

Cuando no se dispone de una red aislada de prueba, es necesario acudir a esta variante. El uso de máquinas virtuales es recomendable cuando se dispone de computadoras con grandes recursos en memoria RAM y velocidad de la CPU

VIOLACIONES COMUNES DE LA SEGURIDAD INTERNA

Cuando se habla de seguridad informática y las medidas de protección a emplear se suele pensar en atacantes externos, en *hackers* profesionales. Hacia ese fin están encaminadas las topologías más comunes de seguridad y las aplicaciones informáticas de protección a la información. Las amenazas internas pueden provenir de diversas fuentes: Empleados descontentos, adolescentes avezados con ansias de demostrar su astucia y conocimientos telemáticos. El desconocimiento, la inocencia y la incapacidad e ineptitud de clientes constituye una amenaza potencial grande a la seguridad de la red.

Analicemos algunas de las amenazas con más incidencia en las redes de nuestra institución..

CORREO ELECTRÓNICO ANÓNIMO

Los márgenes del documento deberán ser simétricos (“mirror margins”), es decir, en las páginas impares el margen izquierdo será el interior y en las páginas pares será el exterior.

Este ataque tiene el objetivo de engañar al usuario destinatario de correo, ocultado la identidad del atacante, se suplanta a un usuario con el fin de empezar a concebir un ataque de mayores proporciones. En los servidores internos SMTP de la red de las entidades educacionales, o en otras, se pueden enviar correos anónimos debido a que este servicio está habilitado en los clientes de correo y no se utiliza la autenticación de este protocolo para enviar el mensaje, sino solo para la descarga.

Un correo anónimo se puede implementar a través de dos métodos principalmente: logrando una conexión Telnet al puerto 25 de un servidor de correo o habilitando el campo “De:” en los gestores de correo como Outlook Express o Microsoft Outlook. Cuando los usuarios utilizan estos clientes de correo y no utilizan opciones como las de cifrado y firmas digitales, todos los mensajes que transmiten por la red son enviados en modo de texto claro, y podrían ser leídos, adulterados o extraída su contraseña utilizando un Sniffer que se mantenga a la escucha el tráfico de la red. Luego será posible la suplantación de identidades.

SNIFFERS

El *Sniffer* [1] es un programa que monitoriza todo el tráfico de la red. Existen dos formas a través de las que puede llevar a cabo su propósito:

Si el *Sniffer* se está ejecutando utilizando la tarjeta en modo normal, podrá chequear el tráfico que va dirigido solo a su dirección MAC.

Si el *Sniffer* se está ejecutando utilizando la tarjeta en modo promiscuo, ésta escucha tanto los paquetes que van dirigidos explícitamente a su estación de trabajo como los que van dirigidos a otras estaciones. En un principio, una computadora no debería trabajar en modo promiscuo a menos que existiera una razón muy poderosa para ello.

Los características principales de un *Sniffer* son: la capacidad de poner a trabajar la tarjeta de red en modo promiscuo, además de descifrar contraseñas y los más avanzados hasta podrían implementar ataques de “envenenamiento” ARP cual será analizado posteriormente.

El *Sniffer* debe trabajar donde se pueda recibir la mayor cantidad de tráfico posible. En un Terminal que se encuentra conectado a un conmutador solo conseguiría escuchar los paquetes que llegan a su máquina, como los de difusión o los que generan sus propias conexiones, pero si se instala en una computadora conectada a un concentrador podría escucharse la comunicación que reciben y envían las computadoras conectadas a ese nodo.

EL PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES ARP

El Protocolo de Resolución de Direcciones *(Address Resolution Protocol*) es un protocolo de bajo nivel utilizado para hacer las direcciones dinámicas. Permite que el cliente que solicita el servicio encuentre la dirección física del cliente destino, en una red física similar, dando solo la dirección IP de éste. Estas direcciones se almacenan en una memoria temporal llamada caché ARP a la que se van incorporando las nuevas direcciones IP a medida que van llegando. El software ARP mantiene las tablas que relacionan las direcciones IP con las direcciones físicas.

Cuando un proceso IP de un cliente fuente está enviando datagramas IP hacia otro cliente, necesita examinar su caché ARP para chequear si tiene almacenada la conversión de dirección IP a dirección física del cliente destino. Si esto sucede, el proceso IP extrae la dirección física, pone los datos en la trama usando dicha dirección y envía la trama. Si no conoce la ruta, debe transmitir una solicitud ARP. Dicho paquete de solicitud es recibido por los procesos ARP de todos los clientes que forman la red (este proceso puede ser complejo porque la otra máquina puede estar sin funcionar o muy ocupada para atender la solicitud, provocando que el emisor no reciba respuesta o que ésta se demore).

El cliente destino reconoce su dirección IP dentro del paquete de solicitud y le envía al cliente fuente un paquete de respuesta ARP con su dirección física. Cuando éste se recibe, el cliente fuente almacena la dirección IP y la dirección física del cliente destino en su caché. Ahora el proceso IP del cliente fuente puede usar la información que está registrada en el ARP de la caché para determinar la dirección física del cliente destino y de esta manera puede entregarle directamente el datagrama.

Para evitar el tráfico innecesario por la red de los protocolos ARP, el emisor debe incluir en cada paquete de solicitud ARP su dirección IP y física. El receptor debe guardar dicha información en su caché antes de procesar el mensaje de solicitud.

El dominio de difusión es diferente en redes con concentradores y conmutadores. En el primer caso las estaciones compiten por el medio y recursos comunes y se reduce considerablemente la velocidad pues comparten 10Mbps y el dominio de colisión. En el segundo caso, al segmentar, el conmutador divide la red en pequeños dominios de colisiones, aumentándose la velocidad y la seguridad en los servidores debido a que la información no se transmite a todas las estaciones, sino solo a aquella con la que se establece la comunicación. Es importante destacar que el tráfico originado por difusión en un dominio de colisiones, será reenviado a todos los demás dominios, asegurando que todas las estaciones en la red se puedan comunicar entre sí.

El conmutador microsegmenta la red en tantos dominios de colisión como cantidad de bocas posee. Para esto mantiene una base de datos con las direcciones físicas MAC de cada interfaz conectada a cada boca, que aprende en forma transparente o automática, cada vez que una computadora se enciende en la

red. Cuando una trama ingresa en una boca del conmutador, este analiza la MAC destino y en base a esa dirección, pasa la trama al puerto donde esta dirección se encuentra.

Entre las medidas, acciones o recursos de seguridad disponibles para un conmutador se encuentran las siguientes:

- Deshabilitar las bocas no conectadas.
- Ingresar las direcciones físicas manualmente.
- Establecer nombres comunitarios de SNMP diferentes de los establecidos usualmente de fábrica.
- Deshabilitar los servicios de administración vía Web
- Establecer cuentas administrativas de acceso diferentes de las establecidas de fábrica.

TÉCNICA DE "ENVENENAMIENTO" ARP

Esta técnica constituye una de las muchas vulnerabilidades del protocolo TCP/IP. La técnica de "Envenenamiento ARP"[2], consigue evitar las propiedades del modo de comunicación de las redes conmutadas (que limitan la difusión de la información). Los conmutadores solo envían información a los clientes que están incluidos en su caché ARP, limitando así la difusión de la información entre el resto de las computadoras de la red. Con el "envenenamiento" ARP se consigue mediante una técnica denominada Man-in-the-Middle[3] u hombre en el medio, falsear la dirección MAC del atacante para poder tener acceso a la información y con un Sniffer capturar los paquetes dirigidos a las demás computadoras.

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

La ausencia absoluta de autenticación en el protocolo: una computadora modificará su comportamiento de acuerdo a los paquetes ARP recibidos ,sin poder determinar de ningún modo la autenticidad de los mismos.

Caches sujetas a alteraciones externas: es posible modificar los contenidos de una caché ARP tan sólo con construir y enviar una petición o respuesta adecuada.

Actualización de las caches a iniciativa externa: con la técnica de ARP gratuito, una computadora puede actualizar las caches ARP del resto en cualquier momento.

Precisamente de estas características se aprovecha la técnica del "envenenamiento" ARP para recibir tráfico ajeno en una red construida con conmutadores. Se basa en "envenenar" la caché ARP de los dos nodos cuya comunicación se quiere intervenir con información falsa, haciéndoles creer que la computadora atacante es su interlocutor. De esta forma, el tráfico generado entre ambas computadoras tiene como destino la computadora atacante, y desde ésta las tramas son reenviadas al destino real, evitándose así la detección del ataque. Más en detalle, un ataque de "envenenamiento" ARP se produce en las siguientes condiciones:

1. La computadora atacante, conociendo las direcciones IP de los dos nodos cuyas comunicaciones se quieren intervenir, resuelve mediante ARP, si es necesario, las direcciones MAC que les corresponden.
2. Bien mediante respuestas ARP o mediante la técnica de ARP "gratuito", el atacante modifica el contenido de las caches de las víctimas de forma que para la dirección IP de su interlocutor se corresponda la dirección MAC real del atacante.
3. Cada vez que alguno de los nodos quiera enviar información al otro, resolverá la dirección MAC del mismo mediante su caché de ARP previamente envenenada, enviando así el tráfico al atacante en vez de al destinatario real.
4. El conmutador enviará las tramas por la boca del destinatario, que en este caso es el atacante. Éste las recibirá y las pasará a la aplicación adecuada, que puede ser un *Sniffer* que capture todo el tráfico. Al estar todas las tramas destinadas a su dirección MAC, no es necesario que la tarjeta de red se encuentre en modo "promiscuo".
5. El atacante reenviará el contenido de las tramas al destinatario real. La única diferencia entre la trama original y la modificada es, en un principio, la dirección MAC del destinatario, que varía entre la del atacante y la de cada una de sus víctimas.
6. El nodo correspondiente recibirá el tráfico como si nada hubiese ocurrido. El atacante, haciendo uso del "envenenamiento" ARP y la técnica del Hombre en el Medio puede interceptar el tráfico sin que los interlocutores o las autoridades informáticas de la red bajo análisis se percaten

Existen muchas herramientas de distribución gratuita en Internet que pueden vulnerar muchos protocolos seguros con el uso de descifradores y así revelar al atacante información que para las políticas de la red estaban seguras. Entre éstas se encuentra Cain&Abel[4], un programa para sistemas operativos de Microsoft que permite recuperar contraseñas. Aunque no es su principal función, utiliza el envenenamiento ARP masivo para capturar el tráfico de la red y recuperar o incluso modificar contraseñas. Es capaz de interpretar múltiples protocolos, incluso VoIP para realizar escuchas telefónicas de forma sencilla.

El "envenenamiento" ARP es considerado como una técnica que puede causar una Denegación de Servicio DoS (*Denial of Service* -) enviando paquetes de respuesta ARP a la computadora de la víctima haciéndole creer que su puerta de enlace predeterminada tiene otra dirección MAC o que el servidor de correo tiene una dirección diferente, denegando así el servicio a los usuarios de la red.

PROPUESTAS DE MEJORA DE LA SEGURIDAD INTERNA DE LA RED

Podría partirse de los ataques que los cortafuegos no pueden detener. Cuando se plantea una topología con cortafuegos, se considera una red interna que debe ser protegida contra los peligros de una red externa. Los cortafuegos no pueden proteger a la red de los ataques que se producen dentro de la

red privada, es decir, ataques que se generan dentro de la misma red, límites en los que el cortafuegos no tiene dominio, en especial cuando la red se comparte entre poblaciones de diferentes intereses vitales.

Para considerar una defensa contra ataques, es necesario abordar el tema desde dos puntos de vista: el uso de mecanismos de seguridad en los terminales (clientes y servidores) y dispositivos de interconexión y la implementación de topologías seguras que doten de protección a las partes más sensibles.

PROPUESTAS PARA LA SEGURIDAD EN LOS CLIENTES

Debido a que la mayoría de los ataques a la red interna están sujetos a la manipulación de la información que los clientes transmiten o reciben por la red, cuando se autentican en servidores, revisan sus correos o utilizan el resto de los servicios, es indispensable dotar de seguridad y privacidad a los clientes para lograr el cumplimiento de las políticas de la red. A continuación se abordan posibles soluciones contra los ataques que se realizan por los clientes.

En los siguientes epígrafes se proponen algunas soluciones que aumentan la seguridad y privacidad de la información tanto de los clientes como la almacenada en los servidores. Igualmente se explica la configuración de un sistema cliente enrutador con seguridad de un cortafuego cliente bastión, que será el elemento principal a utilizar en las propuestas de topologías de seguridad de la red LAN, donde se potencia la seguridad variando la topología.

SEGURIDAD EN EL SERVICIO DE CORREO ELECTRÓNICO

Debido a las vulnerabilidades planteadas anteriormente, es necesario crear políticas en que los clientes suministren seguridad al envío de sus correos. A continuación se proponen dos formas de hacerlo:

Si utiliza gestores de correo, se debe buscar las opciones de cifrado de correos enviados, archivos adjuntos y utilización de firma digital en los correos. A modo de ejemplo en la Figura 1 se explica cómo hacerlo en el gestor de correo Outlook Express:

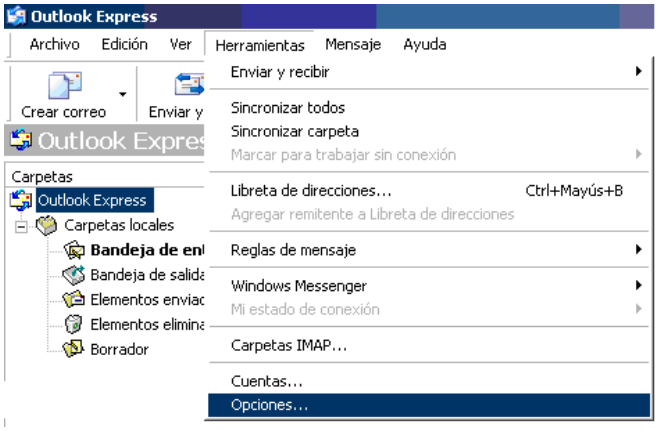

Figura 1 Configuración segura del Outlook Express

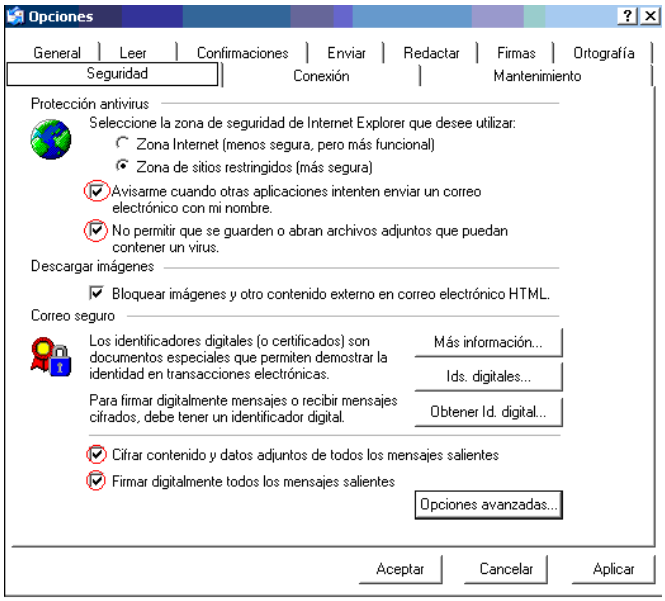

Figura 2 : Configuración segura del Outlook Express

En la Figura 1 se muestra la ubicación de las opciones del programa. En la Figura 2 se muestra la opción de seguridad en la cual los campos que están marcados con rojo son los de especial significación, que permiten cifrar tanto el correo como los adjuntos y firmarlos digitalmente. Cuando se accede a las opciones avanzadas, como se observa en la Figura 3, se encuentran las opciones para enviar correos firmados digitalmente y otras.

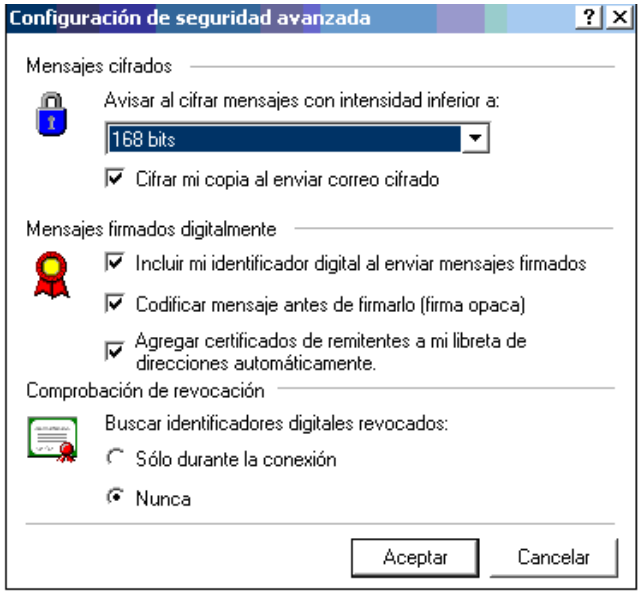

Figura 3 Configuración segura del Outlook Express

Utilizar el correo vía Web (navegadores) como el servicio que presta MDAEMON con su herramienta Web *WorldClient*. Navegadores como el Internet Explorer (navegador diseñado por Microsoft) permite usar el protocolo HTTPS que utiliza SSL para cifrar el contenido de los paquetes y así tener más seguridad en el uso del servicio.

A modo de ejemplo, se podría ver en la Figura 4, la dirección del correo de los profesores de una de las áreas https://fie.uo.edu.cu:8384 en el navegador Internet Explorer y su configuración para permitir el uso del cifrado como protección de la comunicación.

En la Figura 4 se muestran las opciones de seguridad que se pueden implementar en los campos señalados. Nótese como se habilita la autenticación integrada de Windows y el uso de SSL en el navegador.

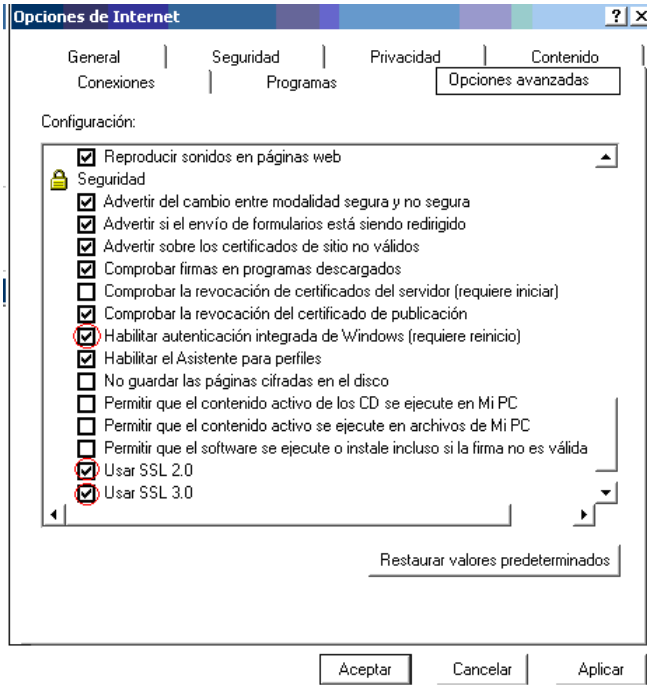

Figura 4: Configuración de Internet Explorer

SEGURIDAD EN CONTRASEÑAS

El primer eslabón débil en la cadena de cómo un cliente podría poner en riesgo la seguridad de la red sería logrando establecer una sesión de administrador en una computadora. Se debe recordar que para instalar aplicaciones que puedan poner en peligro la seguridad de la red, se necesita contraseña de administración y si se olvida prever su importancia podría ser una ventaja esencial para un atacante.
Luego de haber instalado por completo el sistema operativo, se recomienda la configuración del modo de arranque en el Setup de todos los equipos de la red en el siguiente orden:

- HDD (*Hard Drive* – Disco Duro).
- CD/DVD (*Compact Disk / Digital Video Disk*
- Disco Compacto / Disco de Video Digital).
- Disco 3 ½.
- Cualquier otra unidad de almacenamiento

Esta configuración debe ser guardada bajo la seguridad de la contraseña del *Setup*. Esto es debido a que en CDs, discos de 3 ½ y cualquier unidad de almacenamiento, podrían venir implementados programas reveladores y desactivadores de contraseñas de administración del sistema operativo que permitan que los usuarios se apropien del sistema para fines malintencionados.

. Es buena política de red no permitir la escritura por parte de los usuarios en la partición C:\ (en el caso de Windows), pero hay programas que al ejecutarse necesitan la escritura en C:\. Se propone que después de la instalación del paquete de programas necesarios para el trabajo de los usuarios, se agregue un acceso directo en el escritorio de la sesión que

necesite la ejecución de este programa como administrador, y que incluya la sentencia mostrada en la Figura 5.

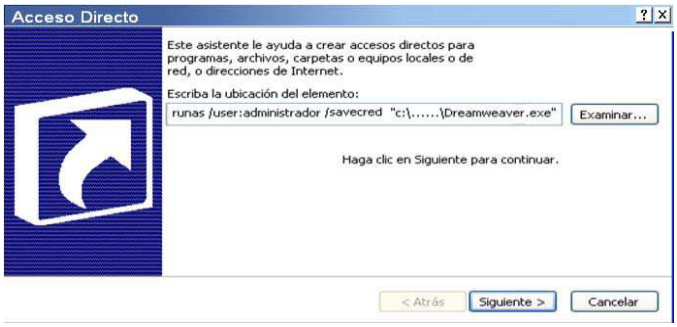

Figura 5 : Implantación del acceso directo

El comando savecred guardará la contraseña de administración en el registro del sistema operativo, por lo que se tiene que poner una sola vez la contraseña de administración en la vida útil del sistema operativo para este fin, de esta forma, solo necesitaría ingresar la contraseña de administrador cuando sea necesario (mantenimiento, instalación de nuevos programas, etc.). También se aconseja que no haya ninguna otra sesión abierta cuando el administrador ingrese al sistema.

Prevención contra el "envenenamiento" ARP y la "suplantación" IP

Existe un mecanismo por el cual una computadora con contraseña de administración podría añadir una entrada a su cache ARP con solo ejecutar en la consola de comandos la sentencia:

arp –s [Dirección IP] [Dirección MAC]

Con esto se logra evitar la suplantación de esta computadora, desactivando cualquier posibilidad de modificación por medio del mecanismo de ARP. Sin embargo, esta sentencia sería temporal, es decir, duraría solo mientras la computadora esté encendida. Una solución más completa es diseñar una base de datos que contenga todas las direcciones IP con sus respectivas direcciones MAC de la red que se va a proteger. Esta aplicación se ejecutaría al principio de sesión en cada computadora. A continuación en Figura 6 se muestra como se implementarían estas entradas, se ha supuesto una subred clase C de tipo 10.30.X.0/24:

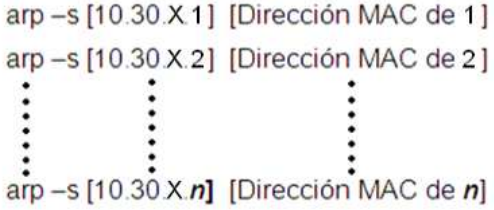

Figura 6 : Implementación de las entradas de la aplicación contra el "envenenamiento" ARP

Aunque la tabla es estática para los usuarios, para el administrador de la red tiene que ser modificable y sería ineficiente que tuviera que modificarse cada cambio en la tabla en cada computadora de la red de la entidad. Por consiguiente, se propone la implantación de dicha aplicación en un servidor de libre acceso de lectura para los usuarios y de manejo del administrador.

En todas las computadoras de la red se implantaría un mecanismo de ejecución (con privilegios de administración) de esta aplicación desde el servidor cada vez que se inicie, sin necesidad de que el usuario este en una sesión con privilegios de administración y automáticamente llene las entradas de a caché ARP de cada usuario. De esta forma se evitará la suplantación de identidad, la sustracción de información ajena y su uso para delinquir. La ejecución que se aplicaría en el inicio de la sesión del SO sería:

net use \\10.30.3.X
runas /user: administrador /savecred
\\10.30.3.X\aplicación.bat

La primera línea conecta al usuario con el servidor que posee la aplicación, en este caso tiene dirección IP 10.30.3.X. La segunda línea es la que ejecuta la aplicación desde el servidor.

Este fichero es un archivo de ejecución por lotes (.bat) y se introduce en la carpeta

C:\Documents and Settings\All Users\MenúInicio\Programas\Inicio

Para aumentar la seguridad de esta base de datos (aplicación) y la comodidad del usuario se compila (*.exe) en modo de segundo plano.

Es de importancia resaltar en que, a través de los métodos de "suplantación" de IP, el atacante ya puede empezar a considerar materializada su intención con el simple hecho de observar el tráfico circulante en la red. Sin embargo, si no puede suplantar identidad en la red no podría llegar a posicionarse en el medio de la comunicación, mucho menos adulterarla y usarla para sus fines. El uso de cache ARP estático dejaría imposibilitado el empleo de estas técnicas en la red conmutada de la red bajo análisis.

PROTECCIÓN DE LOS PUERTOS

Las conexiones entrantes y salientes de las aplicaciones que corren en la computadora s realizan a través de conocidos puertos. Los programas cortafuegos utilizan las comunicaciones por los puertos para defender a las computadoras de conexiones malintencionadas. Por esta razón, es de vital importancia incentivar el uso de cortafuegos en los clientes de la red, con el objetivo de proteger a los usuarios de conexiones a equipos indeseados. La configuración de estas aplicaciones tiene que ser difundida por el administrador de la red.

Un ejemplo de esto es el cortafuegos de Windows XP que constituye un servidor de seguridad que ayuda a mantener más

seguras las computadoras clientes de la red. Éste restringe la información que llega a un equipo procedente de otros (no usuarios), lo que proporciona al cliente un mayor control sobre los datos del equipo y aporta una línea de defensa contra personas mal intencionadas o programas (incluidos los virus) que intentan conectarse a la computadora sin haber sido invitados.

En la Figura 7 se muestra como se puede configurar el cortafuegos de Windows XP Servipack 2 y 3. En ella se muestran las opciones generales del cortafuegos, el cual debe estar activado. En la figura se observan las excepciones a programas o cualquier tipo de conexión externa. Nótese que está activada la opción IPsec lo cual dota a las comunicaciones en la red de una seguridad adicional.

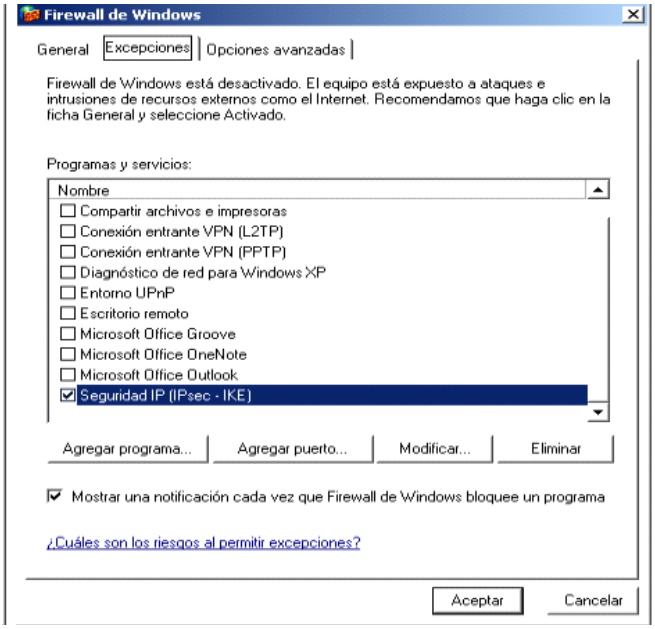

Figura 7: Configuración del cortafuegos de Windows XP

En la figura Figura 8 se muestran las opciones avanzadas del cortafuegos de Windows XP y se observa cómo se pueden elegir los diferentes tipos de conexiones que se van a proteger con el cortafuegos (en este caso la red local). Es de significación destacar el campo señalado que permite configurar los mensajes de control que los usuarios de la red pueden obtener de su computadora.

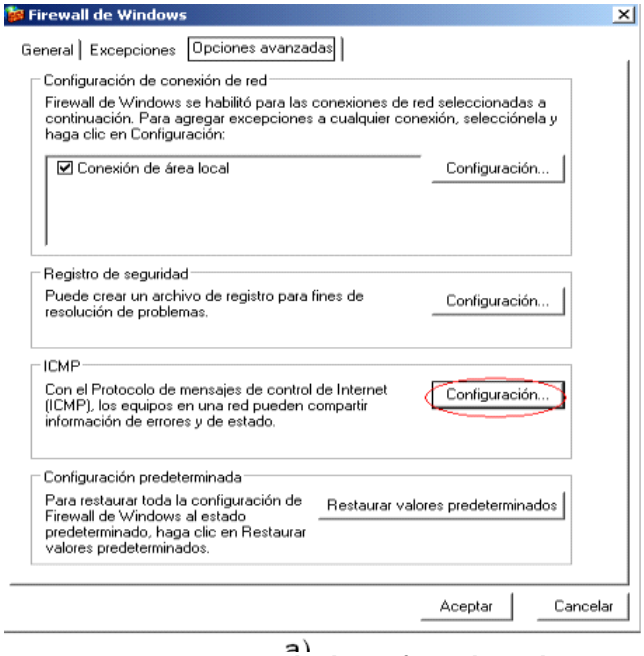

Figura 8: Opciones generales de cortafuegos de Windows XP

En la Figura 9 se muestra como se puede habilitar que su computadora responda a una solicitud de eco entrante.

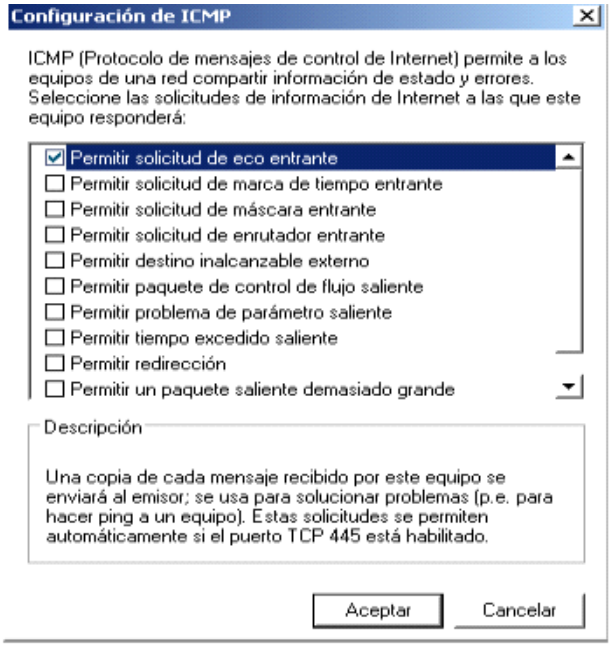

Figura 9: Opciones avanzadas de cortafuegos de Windows XP

PROPUESTAS PARA LA SEGURIDAD EN DISPOSITIVOS DE LA RED Y SERVIDORES

Cuando el cliente transmite información personal al servidor, lo hace por medio de un circuito virtual en el cual la

información no llega a ningún otro cliente en la red. Sin embargo, en una red que usa un concentrador ni siquiera es necesario utilizar "envenenamiento" ARP para sustraer información ya que los datos que intercambia un cliente con el servidor llega a todos los clientes de ese nodo. Esta vulnerabilidad del concentrador pone en peligro a los usuarios pues el simple hecho de que un cliente atacante instale un Sniffer y ponga su tarjeta de red en modo promiscuo, ya implica la sustracción de información ajena en dicho nodo.

La seguridad del servicio de correo

Para la seguridad del servicio de correo es necesario dotar de seguridad estos mensajes haciendo el uso protocolo SSL.. Es importante destacar que procesar páginas con SSL supone una sobrecarga para el servidor que puede reducir su rendimiento. Por este motivo, se recomienda que se aplique SSL de forma selectiva, sólo a aquellas páginas que necesiten cifrado.

DETECCIÓN DE TARJETAS DE RED EN MODO "PROMISCUO"

El uso de una tarjeta de red en modo promiscuo posibilita que un atacante escuche el tráfico en la red por medio de un Sniffer.. PROMISCAN[6] es una utilidad de distribución gratuita diseñada para encontrar las tarjetas de red en modo "promiscuo" muy pesada en la red. PromiScan consigue mostrar cada uno de esos nodos de una manera transparente, claramente visible. En la Figura 10 se muestra la detección de la tarjeta con dirección IP 10.30.3.196 y dirección MAC 00:02:3F:13.FC:13 trabajando en modo "promiscuo".

Figura 10: Detección de tarjeta de red en modo "promiscuo"

Con el funcionamiento de esta herramienta se podría detectar un *Sniffer* que se estuviera ejecutando con tarjeta de red en modo promiscuo. Si la tarjeta de red está en modo normal, no se podrá detectar al atacante.

Detección de intrusos

Un detector de intrusos realiza una monitorización de los paquetes que llegan al equipo e informa cuando detecta un uso anómalo del protocolo, un patrón definido o algo extraño en el comportamiento del equipo que nos envía los paquetes. Esto se puede utilizar para tener una seguridad proactiva y monitorizar en todo momento lo que le está pasando a nuestro sistema. La herramienta que se va a proponer para la detección de intrusos en Windows y en Linux es Snort.

Snort[7] permite hacer una detección de escaneo de puertos, Sniffers, algunos ataques de denegación y rootkits. Además analiza la integridad del sistema por medio de Bitácoras.

PROTECCIÓN CONTRA EL "ENVENENAMIENTO" ARP Y LA "SUPLANTACIÓN" DE IP

Una forma efectiva para lograr este propósito fue mostrada previamente. A este método se le debe agregar la Detección de cambios en direcciones MAC con ARP WATCH[8]

Con las direcciones IP fijas y la relación [IP][MAC] de todas las computadoras y dispositivos de la red, Arpwatch es una herramienta que monitoriza la actividad de red y mantiene esas relaciones es su base de datos. Este programa emite aviso de alerta cuando una tarjeta de red cambia su dirección MAC o con la aparición de nuevos clientes desconocidos, al igual que puede mandarle un correo electrónico al administrador en caso de que esto sucediera. En la Figura 11 se muestra la identificación del cambio de la dirección MAC del cliente LEONARDO con dirección IP 10.30.3.196.

Time	Action	IP Address	MAC Address	DNS Name
10:55:55	Added	10.30.3.196	00:02:3F:13:FC:13	LEONARDO
10:56:01	Added	10.30.3.49	00:04:4B:5A:15:BB	TLM9
10:59:23	HAS CHANGEC	10.30.3.196	00:00:00:00:00:00	LEONARDO

Figura 1 Cambio de dirección MAC

Esta herramienta vigila si una computadora cambia de dirección MAC, pero no puede vigilar las caches ARP de todas las computadoras. Este programa sería una solución para la suplantación de identidad o el cambio de dirección MAC de una computadora, es decir, no solucionaría por completo el uso de técnicas como el "envenenamiento" ARP ni la "suplantación" de IP.

ARQUITECTURA ALTERNATIVA PARA LA PROTECCIÓN BASADA EN HARDWARE Y SOFTWARE

Cuando se debe segmentar la red en situaciones de déficit de presupuesto para la compra de equipamiento de red especializado, como conmutadores gestionables o enrutadores, se puede acudir a la configuración de computadoras como enrutadores, lo cual se conoce como PC-Router[5]

CONCLUSIONES

Cuando un atacante logra ubicarse en el medio de la comunicación entre equipos por la técnica de envenenamiento ARP, puede llegar a interceptar la información, manipularla y materializar ataques más sofisticados ("suplantación de IP")

Se puede asegurar la red sin realizar cambios en su estructura, poniendo en práctica las medidas de seguridad propuestas a nivel de cliente que previenen el "envenenamiento" de la tabla ARP.

El uso del cifrado y monitoreo del canal para asegurar la red, aumentan el tráfico en ésta y disminuyen la eficiencia en la prestación de los servicios.

La implementación de herramientas de monitoreo y detección de intrusos y de comportamientos anómalos de la red puedan

revelar la identidad de personas malintencionadas durante los primeros pasos de sus ataques

REFERENCIAS

[1] **J. FRANKS, P. HALLAM-BAKER, J. HOSTETLER, S. LAWRENCE, P. LEACH, A. LUOTONEN, L. STEWART** " HTTP Authentication: Basic and Digest Access Authentication," June 1999;http://www.rfc-editor.org/cgibin/rfcdoctype.pl?loc=RFC&letsgo=2617&type=ftp&file_forma t=txt

[2] **A. GWINN** " Network Security For Trade Shows," June 1997; http://www.rfc-editor.org/cgibin/rfcdoctype.pl?loc=RFC&letsgo=2179&type=ftp&file_format=txt

[3] **PÉREZ CRESPO, JAIME. "Envenenamiento ARP"** http://blackspiral.org/docs/arp_spoofing.html June 2005.

[4] Cain&Abel http://www.oxid.it/cain.html Sept. 2008.

[5] Implementacion Pc Router. http://www.forocualquiera. com/blogs-del-foro/54710-mi-router-freescoimplementacion- i.html Sep 2008 http://www.taringa.net/posts/linux/1133041/Pc-router-conlinux- suse-10.html Sept. 2008.

[6] PromiScan Download. www.shareup.com/PromiScandownload-20003.html Sep. 2008

[7] Snort Users Manual 2.6.0 http://www.mirrors.wiretapped.net/security/network-intrusiondetection/snort/snort-MANUAL.pdf

[8] ARP WATCH Linux Magazine Online http://www.linuxmagazine.com/issues/2006/73/arp_watch?category=13417

AUTORES

Andrés Subert Semanat Ingeniero en Telecomunicaciones, Profesor Titular del Departamento de Telecomunicaciones y Electrónica de la Universidad de Oriente en Santiago de Cuba.. Avenida de Las Américas s-n CP 90900. Doctor en Ciencias Técnicas desde 1997. Correo: asubert@fie.uo.edu.cu. Teléfono +53(22)646079. Se desempeña actualmente como jefe de la cátedra de Sistemas de Telecomunicaciones. En la mencionada universidad