Amenazas típicas y tipos de ataques básicos en Internet

Resumen

Hay muchas dudas de que ahora sea posible hacer una clasificación completa para todos los ataques reales y potenciales en Internet. Es más, noticias sobre nuevos ataques aparecen periódicamente en publicaciones de los centros de seguridad de la información (CERT, CIAC) de EU.

Por otra parte, los tipos de ataques en redes globales son invariantes con respecto a las características de los sistemas de computación particulares, porque todos los sistemas de computación están diseñados según los mismos principios, usan los mismos protocolos y negociaciones del sistema internacional.

Por lo tanto, podemos considerar las amenazas típicas (aquí el término "amenaza" como una posibilidad para llevar a cabo un ataque) y sus modelos con respecto a la infraestructura de protocolos y su colocación dentro de los niveles lógicos del modelo básico de la red.

Para nuestros propósitos es suficiente mostrar sólo una posibilidad de la clasificación parcial para toda la variedad de los ataques en Internet con respecto a protocolos y servicios comunes, los cuales se usan para su realización.

Amenazas típicas y tipos de ataques básicos en Internet

Para toda la consideración siguiente usaremos la representación de la infraestructura de red global según el estándar internacional ISO 7498-1 (Open System Interconnection. Basic Reference Model).

Aquí hay que hacer unas consideraciones adicionales: Sea una red global que consiste de N objetos de dos tipos (un host $\mathbf{X_i}$, $\mathbf{i=1,\ldots,m}$ y un enrutator $\mathbf{G_j}$, $\mathbf{j=m+1,\ldots,N}$) conectados entre sí por medio de las líneas de la comunicación $\mathbf{K_s}$ en el nivel físico y por medio de líneas lógicas $\mathbf{K_l}$ en el nivel de canal de **OSI**. Hay que notar que en el nivel físico todo el conjunto de objetos de la red se divide en un conjunto de subconjuntos llamados segmentos. Dentro de un segmento todos los hosts interactúan entre sí y con un enrutador correspondiente por medio de las líneas físicas de comunicación bidireccionales (esta consideración se hace para simplificar el análisis de los modelos de ataques típicos, porque en este caso la posibilidad de la comunicación de un host con varios enrutadores dentro de un segmento no influye en el resultado final).

Hay que notar que aunque todos los objetos dentro de un segmento siempre se conectan en el nivel físico, puede ser que la comunicación en el nivel de canal entre ellos exista no para todas las posibles parejas. De tal manera, la comunicación entre hosts de segmentos diferentes será posible solamente a través del enrutador (o a través de una cadena de los enrutadores intermedios).

A nivel de canal cada objeto se caracteriza por medio de sus 48 bits de la tarjeta de la red (nos referiremos a la estructura esparcida de las redes del tipo Ethernet).

En el nivel de la red todos los objetos se conectan entre sí por medio de canales lógicos **Kl** según sus direcciones lógicas de sus 32 bits (IP dirección en Internet). En este nivel (en el modelo de OSI) cada objeto de la red puede comunicarse con cualquier otro objeto remoto por medio de una línea bidireccional o unidireccional de comunicación lógica.

En el nivel **K** del modelo OSI, la comunicación entre dos objetos existe solamente cuando ya existe comunicación en los niveles del 1 hasta el K-1 (K= 1, …, 7), excepto en el caso de que no haya comunicación en el nivel de canal entre dos objetos de un mismo segmento de red, pero exista la comunicación en el nivel de red – llamada esparcida (broadcast) del **ARP** protocolo (del protocolo SAP en los sistemas operativos Novel), la cual es recibida por todos los objetos de un mismo segmento de la red.

Las amenazas típicas en las redes globales son:

- La interceptación e imposición de tráfico y
- Cambio e imposición del enrutamiento.

Estas amenazas se realizan en varios ataques básicos y en cada uno de estos ataques básicos se realizan amenazas potenciales casi siempre en varias combinaciones. Por ejemplo, la interceptación del tráfico común dentro de un segmento se usa para preparar el otro ataque típico del tipo "objeto falso" y este ataque se usa para interceptar el tráfico entre objetos deseados remotos (o locales). A su vez, los ataques básicos se realizan por medio del uso de las desventajas (de punto de vista de seguridad de la información) de protocolos de Internet (RFC 1110) – vea fig 1.

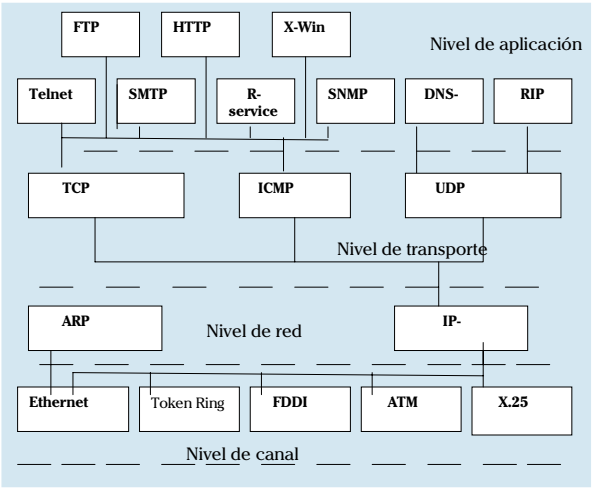

Fig.1 Diagrama de la jerarquía de los protocolos de la red en Internet según los niveles lógicos de OSI (ISO 7498) – del [4].

Aquí observemos brevemente:

En la figura 1 se muestran cuáles protocolos (UDP o TCP) están predeterminados para realizar las aplicaciones dadas. Pero esto no significa que, por ejemplo, el protocolo FTP no pueda basarse en el protocolo UDP.

En el caso común al empezar un proceso de comunicación entre un par de las aplicaciones, en primer lugar se establece un canal virtual (se lleva a cabo en Internet por medio del protocolo TCP), después de unos procedimientos de la autenticación, según de terminología del estándar ISO 7498 se llamará "comunicación en régimen con conexión".

Entonces para realizar cualquier tipo del ataque en este caso hay que superar el sistema de autenticación en el nivel de aplicación y además el sistema de la iden-

tificación de los paquetes TCP (en el protocolo TCP para identificar los paquetes se usan dos números de 32 bits: uno para el número de paquete y otro para el número del canal virtual).

En caso de comunicaciones sin un canal virtual establecido (según la terminología del estándar ISO 7498 - "comunicación sin conexión"), los cuales se usan, por ejemplo, para enviar el mensaje de control de parte de enrutador, etc., la autenticación del objeto se realiza sólo por medio de su dirección IP (lo cual puede cambiarse fácilmente por parte del usuario) y además, para identificar paquetes IP se usa solamente identificador de 8 bits. Esta situación permite enviar mensajes de control falsos, los cuales pueden crear obstáculos graves para el funcionamiento de la red, por ejemplo, pueden cambiar la configuración de red [2].

Aquí es posible distinguir dos tipos de los ataques básicos:

1. Ataques del tipo "interceptación y desviación del tráfico";
2. Ataques del tipo "objeto falso".

1. Amenazas y ataques del tipo "intercepción y desviación del tráfico"

Todos los datos y comandos de control entre las redes se envían por medio de paquetes. Esto, junto con la estructura esparcida de las redes (en los sistemas distribuidos), crea una amenaza a la seguridad de información que se llama "sniffing" (análisis del flujo de tráfico o desviación adicional de tráfico). La amenaza (como un ataque potencial) de este tipo pasivo, en el caso más sencillo, puede ser realizada dentro de un segmento en el nivel físico y no puede cambiar el tráfico. El modelo de este ataque, al tener en cuenta las notaciones anteriores, puede ser presentado como un grafo con los arcos que se corresponden a las líneas de comunicación en el nivel físico de OSI ("sniffing" se realiza sólo dentro de un segmento) – vea la figura 2.

Para este propósito se usan varios programas específicos ("sniffers"), que se llaman a veces "Lan analyser", "Wan analyser", etc., los cuales pueden analizar todo el tráfico y seleccionar paquetes según un criterio dado de antemano, en un segmento de red con la arquitectura esparcida (broadcasting).

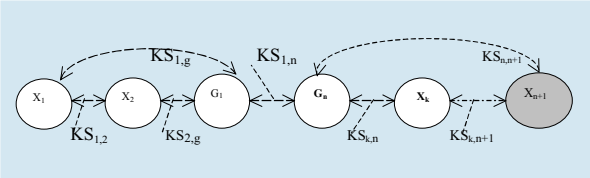

Fig.2 Grafo de comunicación en el caso de una implementación de una amenaza del tipo "sniffing" (en el nivel de canal del OSI).

Por ejemplo en una red Ethernet esto es posible porque cualquier tarjeta de red en una computadora puede ser programada para recibir paquetes Ethernet con cualquier dirección Ethernet.

Como puede verse de este modelo, en el caso común, la realización de esta amenaza se caracteriza por la aparición de un objeto nuevo X_{n+1} y los arcos nuevos $KS_{n,n+1}$ y $KS_{k,n+1}$ en el grafo de la red.

En primer lugar, esta implementación de la amenaza correspondiente permite interceptar y analizar la lógica del funcionamiento de la red local para preparar ataques de cualesquiera otros tipos.

En segundo lugar, en este caso, la intercepción del tráfico entre segmentos permite controlar y analizar el flujo de información entre otros usuarios, en otras palabras, permite recibir acceso no autorizado a la información confidencial de otros usuarios. Por ejemplo en este caso es posible recibir la contraseña y el nombre para acceso a un host en otros segmentos de la red global. En efecto, en Internet los protocolos básicos son FTP (File Transfer Protocol) y TELNET (Virtual Terminal Protocol). TELNET (vea RFC – 1116, RFC – 1205) para conectarse al servidor del host remoto en el régimen de terminal virtual. FTP se usa para la transmisión de archivos entre hosts remotos. En ambos protocolos los usuarios se identifican usando sus nombres y contraseñas, los cuales se envían a través de la red en el modo abierto. En este punto, TELNET descompone la contraseña en símbolos y envía cada símbolo en un paquete diferente. FTP, al contrario, envía la contraseña completa en un paquete. Como resultado, según los datos de los centros de seguridad en computación en EU (CERT, CIAC), en el intervalo 1993-1994 fueron interceptadas cerca de un millón de las contraseñas de acceso a los diferentes sistemas de información[7].

Hay muchas dudas de que ahora sea posible insertar cualquier clasificación completa para todos los ataques reales y potencialmente posibles en Internet [5,6]. Es mas, los avisos sobre ataques nuevos aparecen periódicamente en publicaciones de los centros de seguridad de información (CERT, CIAC) de EU. Pero para nuestros propósitos locales es suficiente dar sólo una clasificación parcial con respeto a protocolos y servicios usados para su implementación (vea la figura 3).

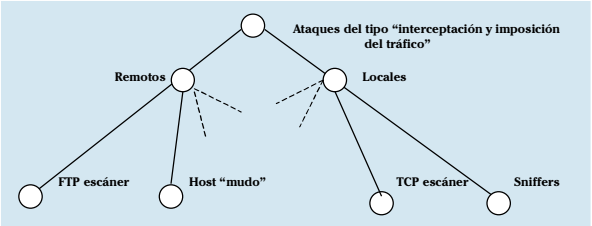

Fig. 3. Clasificación parcial de los ataques del tipo "intercepción y desviación del tráfico".

Los ataques de este tipo remoto se refieren al campo de los ataques reales, los cuales se dirigen para escanear puertos abiertos en hosts remotos.

En realidad, las aplicaciones del servicio remoto, tales como Web, FTP, TELNET, etc., después de que son cargadas, esperan las llamadas remotas de los clientes por conexión en sus puertos correspondientes de TCP (a veces de UDP), los cuales han sido reservados previamente para cada aplicación.

De esta manera, la lista de números de los puertos abiertos (activos) en el servidor significa la existencia de las aplicaciones activas en el servidor, las cuales pueden conceder el acceso remoto.

Para crear una conexión con una aplicación arbitraria, en el primer lugar el cliente debe de crear una conexión TCP con el puerto de TCP correspondiente en el servidor. Para este propósito el cliente envía al servidor el paquete de TCP con el bit SYN establecido – formato del encabezado del paquete TCP se muestra en la fig. 4.

Puerto remitente								Puerto de destino
ID remitente								
ID destino								
Desplazamiento de datos, 4 bits	Reser - vado, 6 bits	U R G	A C K	P S H	R S T	S Y N	F I N	Ventana 16 bits
Checksum (CRC)								Nivel de urgencia
Modificadores								Relleno
Datos								

Fig. 4. Formato de un TCP- paquete (URG, ACK, … son banderas).

Si el cliente recibe una respuesta del tipo TCP SYN ACK, entonces el puerto está abierto y el canal virtual puede ser establecido. Si no hubo respuesta, esto puede significar que el puerto está cerrado, o que el servidor está fuera de servicio.

Después de que el canal virtual ha sido establecido, el cliente y el servidor se intercambian por los comandos específicos para la aplicación dada y la conexión en el nivel de la aplicación de **OSI** se crea.

Hay que hacer notar que el primer paso (la conexión **TCP**) es absolutamente independiente del tipo de aplicación y que está propiedad se usa en todos los métodos para el escaneado de puertos. Todos estos métodos conocidos pueden ser divididos en dos grupos:

1. Escaneado de puertos de manera abierta, cuando el autor se puede identificar por medio de su dirección IP original.
2. Escaneado de puertos en una manera "invisible", cuando solamente se puede detectar la dirección de la fuente intermedia; de esta manera se garantiza el anonimato del autor.

En el primer caso, el método obvio consiste en la transmisión al objeto de TCP SYN–llamadas por conexión, consecutivamente a los puertos diferentes. Como se mencionó anteriormente, si la respuesta es TCP SYN ACK, entonces el puerto está abierto, si respuesta es TCP RST (recuperar conexión), entonces el puerto está cerrado.

Para este propósito puede usarse en lugar de la llamada TCP SYN, la llamada TCP FIN también, pero el uso de esta última posibilidad es más restringido porque algunos sistemas operativos ignoran esta llamada (por ejemplo, Windows).

Hay que notar que ahora existen varios productos de software, los cuales permiten detectar las pruebas de los puertos escaneados, evaluar dirección IP de la fuente y registrar todos los eventos pertinentes. Por lo tanto, este método hay que considerarlo como un método anticuado.

El primer método escaneado del segundo grupo de los métodos de los puertos de manera anónima se llama "FTP Bounse Attack" (ataque encubierto por FTP) y está basado en ciertos detalles sutiles del protocolo FTP (RFC-959).

En general, el cliente de FTP después de la conexión, envía o recibe los archivos solamente por si mismo. Pero este protocolo incluye opciones para realizar conexiones que se llaman "proxy" [3]. Esto significa que cada usuario (incluyendo el anónimo) que está conectado al servidor, puede crear un proceso que se llama servidor DTP (Data Transmision Process) para la transmisión de los archivos a cualquier otro servidor FTP en Internet. Esta característica del protocolo FTP permite realizar el escaneado de los puertos en una manera encubierta por medio del uso de un servidor "proxy FTP".

Después de la conexión con un servidor FTP dado, se envía el comando PORT con atributos de dirección IP y el número de puerto del objeto escaneado. Después, sigue el comando LIST para leer el catálogo correspondiente de este puerto. Todos estas operaciones se realizan consecutivamente para cada puerto.

Hay que hacer notar aquí, que no todas las versiones de servidor FTP tienen "proxy". Por ejemplo, las versiones:

Versión wu-2.4(3), Versión wu-2.4(11), Versión SunOS 4.1 lo tienen, pero las Versiónes DG-2.0, "Microsoft FTP service" Versión 3.0 no.

Hasta finales del año 1998 este fue el único método usado. Ahora también se usan otros. Porque anteriormente el problema más grande para un intruso consistía en la imposibilidad de descubrir la fuente de escaneado por la necesidad de recibir respuestas a las llamadas. Además, los "firewalls" (filtros de paquetes) entre redes a veces podían filtrar llamadas de direcciones IP desconocidas. Por lo tanto, este método revolucionó los métodos de escaneado de puertos porque, primero permitía encubrir la dirección del intruso y, segundo, presentaba posibilidades para escanear el segmento de red protegido por medio de un "firewall" a través de un servidor FTP interno.

El método mas reciente de escaneado de puertos en modo encubierto se llama "Dumb host scan" (escaneado por medio de un host mudo) – vea la fig.5. A grandes rasgos consiste en lo siguiente:

El objeto X_l (vea fig.5a) envía al puerto dado del host X_c la llamada TCP SYN del nombre (del la dirección IP) de host X_m – host "mudo", el host que durante el proceso de escaneado está encendido pero trabaja en modo pasivo (no mantiene ninguna comunicación) – obviamente hay muchos de estos hosts en Internet en un momento dado.

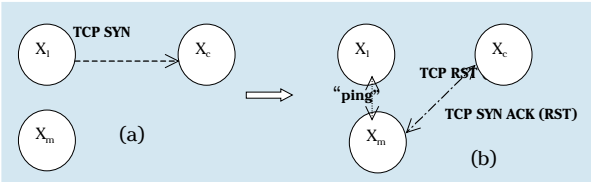

Fig. 5a,b. Escaneado de puertos por medio de un host "mudo".

Si un puerto dado está abierto, el host X_c envía confirmación TCP SYN ACK al host X_m (según la llamada del nombre X_m), si el puerto dado está cerrado, el host X_c envía sólo TCP RST (vea fig. 5b). A su vez, el host X_m respeta a la confirmación "inesperada" por paquete TCP RST (recuperar conexión) e ignora al paquete RST.

Mientras el objeto X_l por medio del programa "hping" (pueden usarse varios tipos del programa "ping") revisa el ID del IP- paquetes provenientes del objeto X_m – vea el formato del paquete IP en la figura 6.

4 bits Versión	4 bits longitud del encabezado	8 bits tipo del servicio	16 bits longitud total
16 bits ID identificador		3 bits banderas	13 bits desplazamiento de los fragmentos
8 bits tiempo de vida	8 bits numero del protocolo		16 bits CRC del encabezado
32 bits dirección – IP remitente			
32 bits dirección – IP recipiente			
32 bits opciones + relleno			
datos			

Figura 6. Formato del paquete IP en estándar de Internet Ipv.4.

Si el ID del paquete IP aumenta consecutivos en uno, entonces X_m se comunica sólo con el programa "ping" y entonces el puerto dado en el objeto X_c está cerrado. Si el ID de uno o varios paquetes IP consecutivos aumenta en dos o tres, entonces X_m envió como respuesta RST y entonces el puerto dado en X_c está abierto.

Amenaza del tipo "rechazo de servicio"

Obviamente que cualquier sistema operativo posibilita mantener sólo el número limitado de canales vir-

tuales abiertos y un número limitado de las respuestas de llamadas (restricciones por la longitud del búfer de llamadas, por la longitud de la cola de las llamadas, restricciones por el número de canales virtuales, por el tiempo para refinar la cola, etc). Estas restricciones se establecen para cada sistema operativo individualmente. Entonces un flujo de llamadas con la frecuencia suficiente puede resultar en un desbordamiento de la cola de llamadas y por lo tanto, en la violación de los funcionamientos del sistema; del rechazo del acceso remoto para otros objetos del sistema y hasta la parada completa de la computadora.

Este tipo de amenaza puede realizarse por dos maneras:

- Un flujo continuo de llamadas de direcciones diferentes con la frecuencia suficiente baja de la capacidad de canal.
- Un flujo continuo de llamadas de una dirección con frecuencia cerca de la capacidad de canal;

El primer caso es más "preferible" y puede realizarse en sistemas los cuales no mantienen procedimientos de autenticación rigurosos (así es en la mayor parte de los casos).

El segundo caso es más restringido, porque la mayoría de los sistemas operativos recientes incluirán varias restricciones para el número (frecuencia) de las llamadas de una dirección.

Estos ataques típicos se llevan a cabo por medio la imposición del tráfico y se usan frecuentemente como una parte auxiliar en ataques del otro tipo. Desde el punto de vista de la tecnología (pero no de la seguridad), todos estos ataques típicos no tienen interés porque se usan las mismas estrategias que en otros tipos, pero casi siempre de manera simplificada.

2. Amenazas típicas del tipo "Cambio e imposición del enrutamiento" y ataques del tipo "objeto falso"

Este tipo de amenaza consiste en la inserción de un objeto adicional intermedio en la ruta de comunicación entre dos objetos en la red para recibir control completo sobre el flujo de información deseado.

El modelo abstracto de la red en este caso puede ser representado por medio de un grafo en la figura 8. En esta figura se muestra el resultado de la realización del ataque "objeto falso" en el caso común, cuando el objeto X_1 se comunica con el objeto remoto X_m en nombre del objeto X_2. En esta situación la topología de la red se cambia de tal manera que en el grafo aparecen dos arcos adicionales: otra línea lógica LS_{2m} unidireccional la cual conecta los objetos X_1 y X_m, y además el camino nuevo KS_{1m} el cual conecta los mismos objetos en el nivel de canal – vea fig.7. Mientras la comunicación entre los objetos X_2 y X_m se lleva a cabo por medio de la línea lógica LS_{2m}, para la cual corresponde el camino físico KS_{2m}.

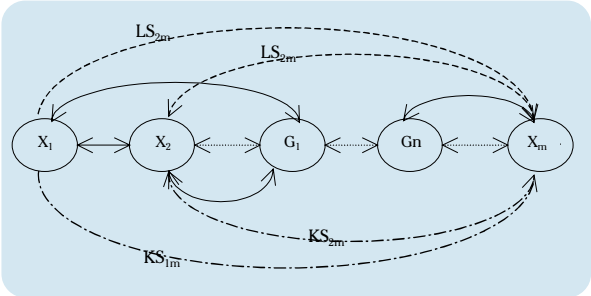

Fig.7. El modelo general para el ataque tipico "objeto falso".

De esta manera, estos ataques del tipo "objeto falso" se acompañan por violaciones a la topología de la red (violación en la concordancia entre los caminos de comunicación en el nivel lógico y el nivel físico) y por lo tanto los "objetos falsos" en este caso no son estables – para mantener tal "objeto falso" hay que llevar a cabo varios acciones adicionales.

Ahora usamos una clasificación parcial para los ataques típicos del tipo "objeto falso" – vea la fig.8.

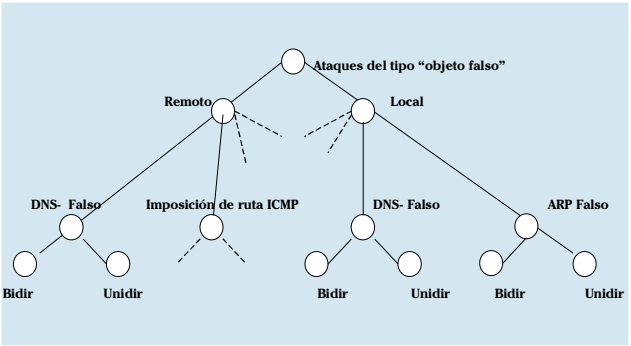

Fig.8. La clasificación parcial de los ataques del tipo "objeto falso".

Como puede verse en esta clasificación, hay dos clases de los ataques del tipo "objeto falso":

- Ataques dentro de un mismo segmento de red (ataques locales),
- Ataques entre segmentos diferentes (ataques remotos).

Ataques dentro de un mismo segmento de red.

El protocolo IP es el protocolo básico para Internet (vea la fig. 6). Pero en el nivel de canal del modelo OSI, el paquete IP se coloca dentro de un paquete Ethernet (así como un paquete TCP se coloca en el campo de datos de un paquete IP). Por lo tanto, cada paquete en las redes de cualesquier tipo con cualesquiera protocolos finalmente se envían a la dirección de la tarjeta de red la cual recibe y envía paquetes directamente.

Entonces, para dirigir un paquete a un host dentro de un segmento de red, además de su dirección IP, hay que tener su dirección Ethernet o, en caso de comunicación entre segmentos, hay que tener la dirección Ethernet del enrutador. Puede ser que un host (por ejemplo, nuevo) no tenga la información sobre la dirección del enrutador o de otro host nuevo. Para resolver estos problemas se usa el protocolo ARP (Address Resolution Protocol), el cual permite recibir la concordancia necesaria entre las direcciones IP y Ethernet para cada host dentro de un segmento de red. En este caso un host emprende los siguientes pasos:

- Envía una llamada esparcida a la dirección Ethernet ffffffffffffh con la dirección IP del enrutador (la dirección IP del enrutador se le asigna a cada host durante el proceso de instalación del sistema operativo) la cual recibirán todos los hosts dentro de este segmento, incluyendo el enrutador.
- En el enrutador está almacenada toda la información en una tabla especial con las parejas de direcciones IP y Ethernet para cada host dentro del segmento dado. Después de que fue recibida tal llamada, el enrutador aumenta su tabla de direcciones ARP con un registro adicional con las direcciones IP y Ethernet del nuevo host y después envía la respuesta al nuevo host con su dirección Ethernet.
- A su vez, si el host nuevo reciba una respuesta del enrutador, escribe está información en su propia tabla de direcciones ARP.

Todos estos pasos se realizan de manera semejante en el caso de una búsqueda por la dirección Ethernet de cualquier otro host dentro de un segmento.

Como resultado, después de un corto tiempo cada sistema operativo dentro de un segmento dado puede obtener toda la información sobre la concordancia de las direcciones dentro de este segmento.

Un ataque típico del tipo "objeto falso" dentro de un segmento -"ARP servidor falso" se realiza por medio de la intercepción de la llamada esparcida y de la transmisión de la respuesta falsa ARP – fig.9 a,b.

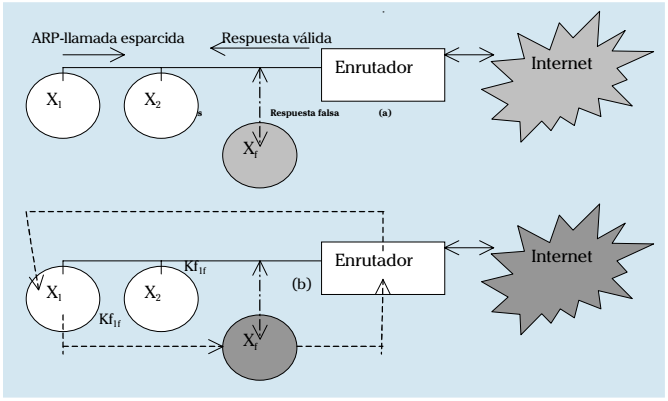

Fig.9a, b. Esquema de un ataque típico "ARP servidor falso".

En esta figura supongamos que el objeto X_1 envía una llamada esparcida ARP al enrutador, el objeto X_f recibe esta llamada (como todos los objetos dentro del segmento dado) y enseguida envía la respuesta falsa, que ha sido preparada anteriormente, con el nombre del enrutador al objeto X_1.

La respuesta falsa de X_f, en este caso, incluye la dirección Ethernet del objeto X_f en lugar de la dirección Ethernet del enrutador. Luego, si el objeto X_1 percibe una respuesta falsa, la configuración de red se cambiará de tal manera que todos los paquetes del objeto X_1 han de pasar por un camino nuevo Kf_{1f} que pasa a través del enrutador falso – el objeto X_f (línea punteada en la figura 9b).

Mientras que todos los paquetes que llegan de afuera al objeto X_1 a través del enrutador estarán siendo enviados al objeto X_1, por lo que se ha dicho anteriormente, las direcciones IP y Ethernet del objeto X_1 fueron escritas en la tabla de ARP cuando el enrutador recibió la llamada esparcida del objeto X_1. Por lo tanto, este acercamiento no puede crear (como

se ha discutido anteriormente – vea la fig.7 y el texto correspondiente) el "objeto falso" estable y recibir interceptación completa del flujo de la información del objeto X_1.

Hay varias posibilidades para recibir intercepción completa en este caso. El método más eficaz consiste en lo siguiente:

El objeto X_f puede seguir más adelante y enviar su propia llamada ARP al enrutador para cambiar su dirección IP por cualquier dirección IP libre dentro el grupo de direcciones IP de este segmento. Obviamente, en esta llamada hay que indicar la dirección Ethernet del objeto X_1 (la dirección Ethernet en tarjeta de red puede cambiarse por medio de programación en el ámbito de la tarjeta API). Entonces en este caso todo el flujo de información al objeto X1 y así mismo del objeto X1 estará pasando a través del servidor falso ARP. De tal manera este acercamiento crea un "objeto falso" estable y esta tecnología coincide casi completamente con una tecnología bien conocida, la cual se usa en "servidor proxy".

Aquí hay que notar adicionalmente:

- El objeto X_f en este paso podría cambiar su dirección IP por la dirección IP del objeto X_1, en este caso no puede conservar su transparencia, porque casi todos los sistemas operativos recientes detectan este evento y envían un mensaje con la advertencia "Está dirección IP ya está siendo usada en el sistema" (envían mensaje pero no impiden).
- Lo que se ha dicho anteriormente sobre "servidor falso ARP" se refiere sólo a las posibilidades dentro de un segmento de la red, y una amenaza del tipo "objeto falso" puede ser llevada a cabo en este caso muy fácilmente en él porque el protocolo ARP no contiene procedimientos para autentificación excepto el de la dirección IP, el cual puede ser cambiado muy fácilmente.
- La eficacia de este tipo de ataque depende parcialmente de la especificación en la organización del servicio ARP dentro de los diferentes sistemas operativos:

  Linux (UNIX) envía una llamada ARP sólo cuando su tabla interna ARP no incluye la dirección Ethernet deseada.

  Win 95 también envía una llamada ARP sólo cuando su tabla interna no incluye la dirección Ethernet deseada, pero periódicamente(cada minuto) envía una llamada al enrutador por su dirección Ethernet, entonces en caso de este ataque, después varios minutos puede este sistema operativo ser controlado completamente por el "servidor falso ARP";

  WinNT – casi lo mismo, sólo que envía llamadas ARP cada cinco minutos.

  Sun5.3 envía una llamada ARP cada vez que establezca comunicación con algún host dentro del segmento.

Ataques remotos del tipo "objeto falso"

Estos ataques comúnmente son más difíciles desde el punto de vista técnico si se comparan con los locales.

Desde el punto de vista del usuario cada host en Internet tiene su nombre, pero la comunicación en redes se realiza por medio de la dirección IP única de 32bit para cada host en Internet. El sistema que actualmente se usa en Internet para transformar los nombres en las direcciones IP correspondientes se llama DNS (Domain Name System) y él se mantiene por medio del protocolo DNS (vea RFC-1101). El algoritmo del protocolo DNS que se usa para una búsqueda remota de una dirección IP a partir del nombre del host deseado incluye los pasos siguientes:

- El host dado envía una llamada DNS dirigida a la dirección IP del servidor DNS más cercano (su dirección IP se ha escrito en sistema operativo de red en el proceso de instalación). Está llamada incluye el nombre del host, cuya dirección IP fue solicitada.
- El servidor DAS recibe está llamada, busca en su base de nombres este nombre y si la búsqueda se termina con éxito, entonces envía la respuesta al host dado. Si el nombre deseado no existe en su base, entonces a su vez envía una llamada al servidor DNS en el nivel inmediato superior en jerarquía de los servidores DNS. Si fue recibida una respuesta, el servidor DNS escribe estos datos en su base y envía la respuesta al host dado.

Ataque del tipo "DNS-servidor falso"

En tiempo reciente existen tres posibilidades para realizar un ataque de este tipo:

Antes de considerar el algoritmo de un ataque a un servicio DNS hay que prestar atención a varias sutilezas del protocolo DNS.

En primer lugar, el protocolo DNS usa el protocolo UDP que no incluye procedimientos para autentificación de los objetos de comunicación (vea la fig.10).

Nombre del remitente
Número del puerto remitente
ID identificador de la llamada
IP- dirección del DNS- servidor
IP- dirección del remitente

Fig.10. Estructura de la información en un paquete UDP de una llamada DNS.

En segundo lugar, cualquier sistema operativo de red exige que:

1. En la respuesta del servidor DNS la dirección IP del remitente ha de coincidir con la dirección IP del servidor DNS.
2. El nombre en la respuesta DNS ha de coincidir con el nombre en la llamada DNS.
3. El número del puerto UDP ha de coincidir con el número en la llamada DNS.
4. El valor de ID en la respuesta ha de coincidir con el valor ID del remitente (vea la fig.10).

Por lo tanto, para realizar este ataque por medio de intercepción de una llamada DNS hay que usar toda la información del paquete interceptado (según los puntos 1-4) para formar una respuesta DNS falsa con su propia dirección IP en lugar de la dirección IP del objeto solicitado – vea la fig.11a.

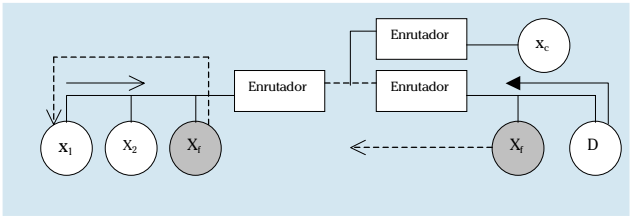

Fig.11a. Esquema de un ataque "DNS-servidor falso".

Aquí:

Objeto "D" – servidor DNS.

→ - llamada DNS- del objeto X_l por la dirección IP del objeto X_c.

⇢ - respuesta DNS falsa del objeto X_f al objeto X_l.

⟶ - respuesta DNS válida del servidor DNS.

En la figura 11a pongamos que el objeto X_l tiene que comunicarse con el objeto remoto X_c y con este propósito llama al servidor DNS para recibir la dirección IP del objeto deseado. El objeto X_f tiene la posibilidad de interceptar una llamada DNS dirigida sólo en los casos de que esté en el mismo segmento que X_l o de que esté en el mismo segmento que un servidor DNS. En estos casos X_f intercepta está llamada y después envía una respuesta falsa del nombre del servidor DNS al X_l.

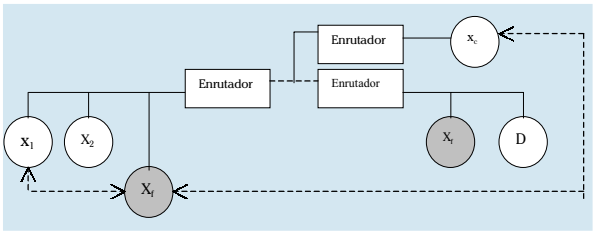

Fig.11b. Esquema de un ataque "servidor falso DNS" la información fluye (línea puntada) a través de X_f (DNS- servidor falso).

Si X_l percibe esta respuesta falsa, entonces la estructura de comunicación en la red cambiará de tal manera que todo el flujo de la información entre los objetos X_l y X_c estará pasando a través del servidor falso – vea la fig.11b.

Obviamente que en este caso el objeto X_f también no será estable y para guardar el control del flujo de la información deberá cambiar su dirección IP por la dirección IP del objeto X_l para todos los paquetes de X_l al X_c y viceversa.

En realidad cuando el cliente FTP se conecta con el servidor remoto FTP, después de cada comando FTP escrito por el usuario del tipo "get", "put", etc., el cliente FTP produce el comando "PORT" el cual envía al servidor FTP en el campo de datos del paquete TCP el número de puerto y la dirección IP del cliente. Por lo tanto, si la dirección IP del objeto X_l no se cambia dentro del objeto X_p, entonces el siguiente paquete del servidor se enviará al objeto X_l directamente y por lo tanto X_f perderá su control sobre la comunicación entre X_l y X_c.

Esta posibilidad para la realización de un ataque de este tipo existe porque el servidor FTP no tiene ninguna posibilidad para la autenticación de clientes y supone que todos los procedimientos de autenticación se realizan al nivel de protocolo TCP.

Realmente este esquema de ataque es muy raro porque comúnmente el objeto X_f se coloca en cualquier otro segmento de red y no tiene ninguna posibilidad para interceptar la DNS- llamada dirigida.

Imposición de una DNS- respuesta falsa

En este caso (X_1, X_f y el servidor DNS se colocan en segmentos diferentes) el objeto X_f envía al objeto X_1 una serie continua de respuestas falsas, las cuales han sido preparadas previamente a nombre del servidor DNS (X_f no sabe cuándo X_1 enviará su llamada DNS). Este método de actuación es posible porque para llamadas DNS se usa el protocolo UDP, que no incluye procedimientos para autentificación de paquetes.

Pero ahora X_f no puede interceptar una llamada DNS y por lo tanto deberá resolver el problema principal con el número de puerto y el número ID en el paquete UDP de X_1 (vea la estructura de un paquete UDP presentada en la fig.10) para construir su respuesta DNS falsa. Pero se encuentra que este problema realmente no es tan difícil:

El número de ID en un paquete UDP depende de la aplicación que produce la llamada DNS – si está llamada es enviada por el sistema operativo de un host (Linux o Win95, por ejemplo), entonces el valor del ID siempre será igual a uno, si está llamada se envía por Netscape o por un DNS- servidor, entonces para cada llamada siguiente el número ID en el paquete UDP se aumenta por uno. Luego es más probable que el número de ID esté entre uno y diez.

El valor inicial del número del puerto UDP (puerto remitente – vea la fig.10) debe de ser mayor que 1023 (para aplicaciones) y éste se incrementa en uno por cada llamada DNS nueva.

Al tener en cuenta estos detalles, el esquema de ataque en este caso pueda ser representado por fig. 12.a,b.

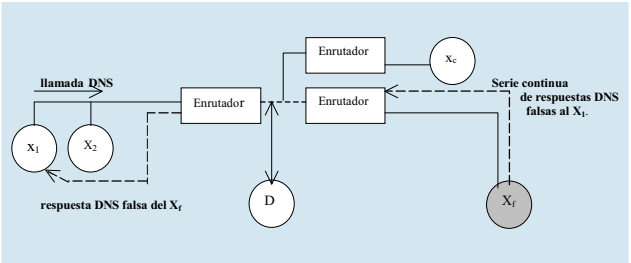

Fig.12a. Esquema del ataque "servidor falso DNS". Aquí el Objeto "D" es un servidor DNS.

En la fig.12a, X_f envía una serie de respuestas DNS falsas al objeto X_1 del nombre (de la dirección IP) del servidor DNS en la que se indica la dirección IP del objeto X_f en lugar de la dirección IP del objeto X_c. Esta serie incluye paquetes UDP con varias combinaciones de números de ID y puertos del remitente según nuestra discusión anterior.

En esta situación, si X_1 enviará su llamada DNS, enseguida recibirá la respuesta falsa de la serie continua de respuestas falsas. Desde este momento el sistema operativo de X_1 considerará X_f como objeto X_c y por eso el flujo de la información entre X_1 y X_c pasará a través del objeto falso X_f – vea fig.12.b.

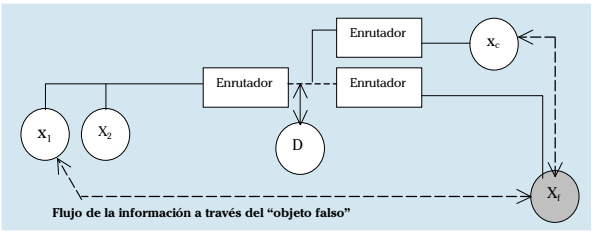

Fig.12b. Esquema del ataque "servidor falso DNS". Aquí el Objeto "D" es un servidor DNS.

Aquí hay que hacer notar lo siguiente:

Para el éxito de tal tipo de ataque hay que garantizar que el objeto X_1 recibirá una respuesta DNS falsa antes de una respuesta DNS válida del servidor DNS. Con este propósito usualmente X_f genera simultáneamente a las respuestas DNS falsas una serie continua de llamadas DNS al puerto 53 (número de puerto UDP predeterminado en el servidor) para crear una sobrecarga en su cola de llamadas.

Para mantener el control sobre el flujo de la información ("objeto falso" no estable), el objeto X_f en caso de recibir un paquete del objeto X_1 ha de cambiar la dirección IP de X_1 por su propia dirección IP antes de enviar este paquete al objeto X_c y viceversa, ha de cam-

biar la dirección IP en paquete de X_c por su propia dirección IP antes de enviarlo al objeto X_1.

Intercepción de una llamada de un servidor DNS

Como se ha dicho anteriormente, si el servidor DNS local no encuentra en su base el nombre deseado, entonces envía su propia llamada DNS dirigida a uno de los servidores DNS en el nivel inmediato superior de la jerarquía. Obviamente que en este caso el esquema de ataque anterior puede ser cambiado de tal manera que la serie de respuestas DNS falsas se envían a través del objeto X_f al servidor DNS local del nombre (del la dirección IP) de un servidor DNS inmediato superior (en la jerarquía de los servidores DNS).

Aquí hay que tener en cuenta que cada servidor DNS mantiene su base de concordancia entre nombres y direcciones IP en el modo de "cash – tabla".

Esta tabla se mantiene dinámicamente sobre cambios continuos y nombres nuevos entre los objetos de la red. De tal manera que si el servidor DNS recibe una respuesta a su llamada, escribe este par nuevo con el nombre y su dirección IP en su tabla de direcciones para no hacer búsquedas adicionales en caso de llamadas repetidas – vea fig. 13.

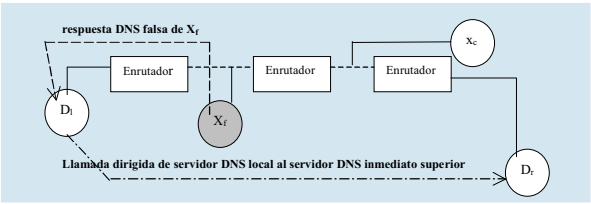

Fig. 13. Imposición al servidor DNS local de la respuesta falsa del servidor inmediato superior Aquí: D_l servidor DNS local; D_r servidor DNS- inmediato superior.

Es obvio que en el caso de flujo continuo de respuestas falsas DNS al servidor DNS, en las cuales se indica la dirección IP del objeto X_f por el nombre del objeto X_c, después de un cierto tiempo en la tabla de direcciones del servidor DNS se encuentra un registro con esta información falsa.

Pero comúnmente X_f no puede interceptar llamadas DNS directamente si se coloca en un segmento de red arbitrario. Por eso el objeto X_f para construir una respuesta falsa para la llamada DNS correspondiente tendrá que resolver el problema con el número ID de un paquete UDP de la llamada DNS (el número de puerto remitente en el servidor DNS como se ha notado anteriormente está predeterminado y tiene el valor 53).

Este número de ID se incrementa en uno para cada llamada consecutiva y en este caso X_f ha de cambiar el número ID sucesivamente entre 0 y 2^{16}.

Comúnmente el servidor DNS envía su llamada DNS sólo después de la llamada de un host arbitrario el cual incluye un nombre desconocido. Para evitar una espera indefinida X_f desde su dirección IP envía una llamada DNS solicitando el nombre del objeto deseado a fin de provocar al servidor DNS para una búsqueda remota – vea fig.14.

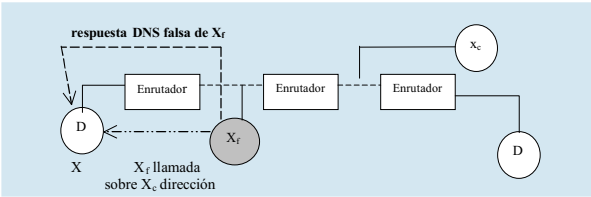

Fig. 14. X_f provoca al servidor DNS local con una llamada DNS para que este servidor envíe una llamada DNS al servidor DNS inmediato superior. Aquí: D_l – servidor DNS local; D – servidor DNS inmediato superior.

Ataques de este tipo pueden realizarse sólo debido a fallas en la seguridad en el servicio DNS y pueden violar el enrutamiento entre cualquier par de objetos en Internet de cualquier parte de la red global.

Los resultados de ataques de estos tipos son muy peligrosos porque la información falsa escrita en la base de servidor DNS será difundida entre otros servidores DNS en Internet [2].

"Objeto falso" por medio de imposición de ruta falsa por ICMP

El enrutamiento en Internet se realiza en el nivel de red (nivel IP) según la estructura de OSI. Dentro de cada sistema operativo en red existen tablas especiales incluyendo los datos sobre rutas diferentes. Dentro de un segmento todos los mensajes dirigidos hacia fuera del segmento se envían al enrutador, el cual los reenvía más adelante según la dirección IP de la ruta óptima.

Todos los enrutadores en la red global tienen tablas específicas del enrutamiento, las cuales incluyen para cada dirección IP una lista de nodos intermedios óptima. Para manejar el enrutamiento se usan protocolos específicos: RIP(Routing Internet Protocol), OSPF(Open Shortest Path First) – [1].

Notificaciones a los hosts sobre rutas nuevas se realizan por medio del protocolo ICMP (Internet Control Message Protocol). El control remoto por enrutadores se realiza por medio del protocolo SNMP (Simple Network Management Protocol, vea RFC- 1089). Todos estos protocolos permiten cambiar el enrutamiento remotamente, y por lo tanto son protocolos de control de red global.

Cada tabla de enrutamiento dentro del sistema operativo en el host consiste de cinco columnas:

- Dirección IP
- Máscara de red
- Dirección del enrutador
- Interfaces
- Métrica

Además, usualmente el sistema incluye una ruta predeterminada (cuyo campo correspondiente a la dirección IP tiene solamente ceros y el campo correspondiente al enrutador tiene la dirección IP del enrutador). De esta manera todos los paquetes que se envían fuera del segmento dado serán enviados por esta ruta predeterminada.

Como es bien conocido uno de los mecanismos del ICMP- protocolo es el control remoto de la tabla de enrutamiento en los hosts dentro de un segmento dado. Este mecanismo ha sido diseñado para evitar las transmisiones de mensajes a través de rutas no óptimas, y además para mejorar la fiabilidad de redes cuando un segmento tiene más de un enrutador. Por ejemplo, puede ser que una ruta sea corta a través de un enrutador, pero por otra dirección la ruta es más corta a través de otro enrutador y además cuando un enrutador está descompuesto, la comunicación con Internet será posible a través de otro enrutador.

El control remoto del enrutamiento en la red local se realiza por medio de la transmisión del aviso ICMP "redirect message" (mensaje para el redireccionamento) del enrutador al host. La estructura del encabezado de este mensaje se muestra en la fig.15.

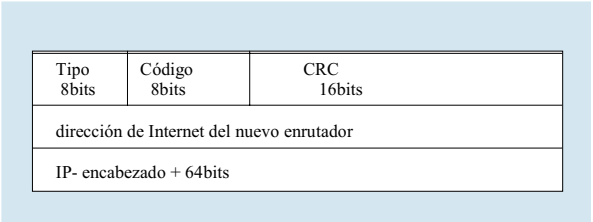

Fig.15. Encabezado del aviso ICMP "Redirect Message".

El contenido de lo campos es como sigue:

- El tipo: es igual a cinco (número de protocolo)
- El código: 0- "redirect datagrams for the Network"

1 – "redirect datagram for the host", 2 – "redirect datagrams for the type of service and Network", 3 – "redirect datagrams for the type of service and host".

Como se sigue de la especificación del protocolo ICMP, el código "0" indica al host que debe de cambiar la dirección del enrutador que le fue predeterminado, o indica que debe de cambiar la dirección a otra subred.

Código "1" informa al host que debe de crear una ruta nueva hacia el objeto mencionado en el mensaje, e insertarlo en la tabla de enrutamiento (la dirección del host, para lo cual es necesario un cambio del enrutamiento, será escrita en el campo "destino" dentro del encabezado del paquete IP asociado). La dirección IP nueva del enrutador para el host mencionado se escribe en el campo "dirección de Internet..." (vea la fig.15).

Según los datos de las publicaciones dedicadas al protocolo ICMP (RFC - 1089), el mensaje con el código "0" es anticuado y no se usa en los sistemas operativos recientes. Mientras que los mensajes del protocolo ICMP con el código "1" son válidos para los sistemas operativos Win95 y Win NT, y no son válidos para los sistemas operativos recientes del tipo UNIX (Linux). EL análisis del mecanismo de la autentificación en el protocolo ICMP indica que el único atributo, que se usa para autentificar el mensaje "redirect", es la dirección IP del remitente. Esta dirección IP ha de coincidir con la dirección IP del enrutador, porque un aviso de este tipo puede enviarse por parte del enrutador. Por lo tanto nada impide a cada usuario enviar el aviso "redirect" del nombre (de la dirección IP) del enrutador más cercano.

Hay dos posibilidades para realizar los ataques de este tipo:

- El cambio del enrutamiento dentro de un mismo segmento, y
- El cambio del enrutamiento desde afuera de un segmento.

En el primer caso el esquema del ataque se muestra en la fig.16.

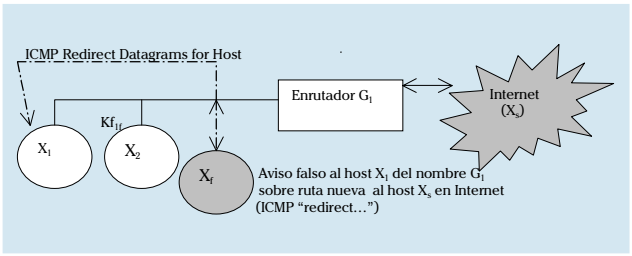

Fig.16a. Esquema de un ataque típico "ICMP redirect...".

En primer lugar el objeto X_f envía un aviso del nombre "ICMP redirect datagrams for host" al host X_1 (de la dirección IP) del enrutador, en el que se indica su dirección IP como dirección IP del enrutador nuevo (en este caso es mejor usar la de cualquier dirección IP libre del grupo de direcciones IP en este segmento). En el caso de éxito, la tabla de enrutamiento dentro de X_1 se cambia de tal manera que la ruta al host X_s pasará a través del enrutador falso X_f – vea fig.16b.

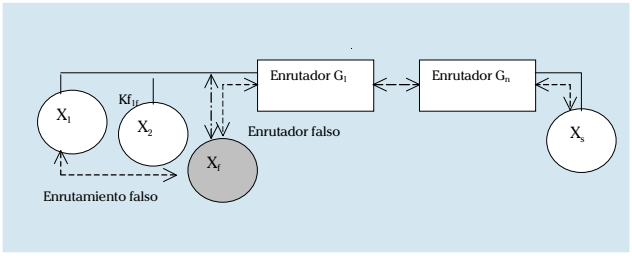

Fig.16b. Esquema del resultado de un ataque típico "ICMP redirect..." para la inserción de un enrutador falso.

Si el host X_1 envía una llamada ARP solicitando la dirección Ethernet de este nuevo enrutador, X_f envía una respuesta falsa con su propia dirección Ethernet.

Si X_f recibe un paquete del host X_1, entonces envía este paquete al enrutador real G_1.

Si X_f recibe un paquete del host remoto X_s, entonces envía este paquete al host X_1.

En el caso común X_f puede atacar a cualquier host de cualquier segmento de la red global y por lo tanto no tiene posibilidad de controlar el tráfico entre X_1 y X_s, porque el enrutador falso y el enrutador real deben de pertenecer al mismo segmento. Es decir, en este caso X_f no puede recibir acceso al flujo de la información entre X_1 y X_s. Pero, por medio de un ataque de este tipo X_f puede violar la comunicación entre los objetos mencionados.

El esquema de un ataque remoto por medio del uso del procedimiento "ICMP Redirect ..." se muestra en fig. 17.

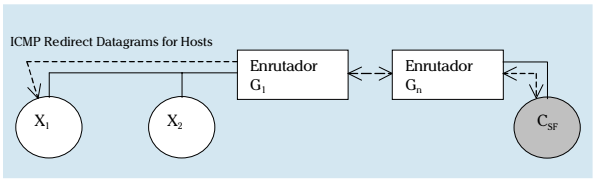

Fig.17a. Esquema de un ataque típico "ICMP redirect..." en la manera remota.

En este caso el objeto X_f desde cualquier lugar en Internet puede enviar el aviso "ICMP Redirect ..." al objeto X_1 en el que se indica la dirección IP de cualquier host del mismo segmento que X_1 como la dirección IP del enrutador nuevo. Si el sistema operativo de X_1 percibe este aviso, entonces la comunicación del objeto X_1 se viola – vea fig.17.b.

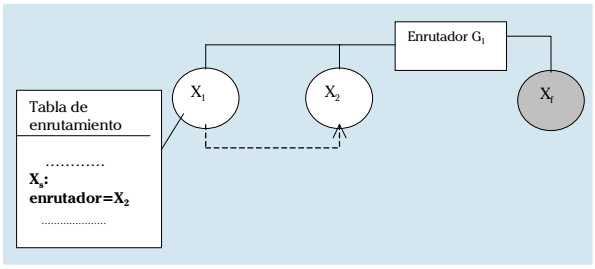

Fig.17b. El esquema del resultado de un ataque típico "ICMP redirect..." de la manera remota (vea el texto).

Esta violación de la comunicación del objeto X_1 sucede porque la tabla de enrutamiento en X_1 ahora incluye un registro con la ruta falsa, en lugar de la dirección IP del enrutador se indica la ruta al host arbitrario X_2 - vea fig. 17b.

Aquí hay que hacer varias observaciones:

De lo que se ha escrito anteriormente se desprende de que para realizar un ataque de este tipo, X_f debe de resolver dos problemas:

En primer lugar hay que tener la dirección IP interna del enrutador G_1. Desde la red externa sólo es posible encontrar la dirección IP externa del enrutador G_1 (por ejemplo, por medio del uso del programa "traceroot"). Si suponemos que la red local dada pertenece a la clase C (como la mayoría de las redes locales), entonces X_f ha de enviar a lo más 256 avisos "ICMP Redirect...".

En segundo lugar, el objeto X_f ha de escoger el nombre (o dirección IP) del host, el cual estará usando para el cambio de enrutamiento. Generalmente para este propósito se usan nombres de servidores bien conocidos, por ejemplo, de los servidores de empresas famosas, de los sistemas para la búsqueda en el Internet, etc.

La causa de tal situación en el campo de la seguridad es que hasta ahora en Internet (IPv.4 estándar) se usan protocolos que fueron diseñados en años 60-80, antes de que las computadoras personales aparecieran. Ahora para cada individuo hay disponible una computadora tan poderosa como las más poderosas de esa época y además cada individuo tiene disponible acceso casi irrestricto a la red global creando una situación de los sistemas de computación que no tiene precedentes.

Actualmente existen varios protocolos de comunicación, que permiten proteger el canal virtual y encriptar el tráfico completamente (por ejemplo, SSL, SKIP, PPTP, etc.) [1], pero éstos no han reemplazado a los anteriores y todavía no están incluidos en el estándar para Internet (con excepción del protocolo SSL, pero este protocolo sólo se usa en algunas transacciones de Web). Posiblemente la situación de la seguridad en Internet mejorará después de la introducción del nuevo estándar para Internet IPv.6

Referencias

1. Nike D.
1999 "Standards and protocols in Internet", M, Channel Trading Ltd.

2. Bellovin S.
1989 Security problems in the TCP/IP- protocol suit. Computer communication review, 2:19, p. 32-48.

3.CIAC information bulletin E-17. FTP Daemon vulnerabilities.

4. Medvedovsky I., Semianov P., Leonov D.
1999 Attacks on Internet. M.

5. Landwerr G.E. and oth.
Taxonomy of computer security flaws with examples. Information technology division, Code 5542, Naval Research Laboratory, Washington, D.C. 20375-5337.

6. Ranum M.
Taxonomy of Internet attacks.
http://www.clarc.net/pub/mjr/pubs/attck/index.html.

7. 1997 CIFS: Common Insecurity fail scrunity.

Yury Paramonov Victorovich
Universidad Tecnológica de la Mixteca