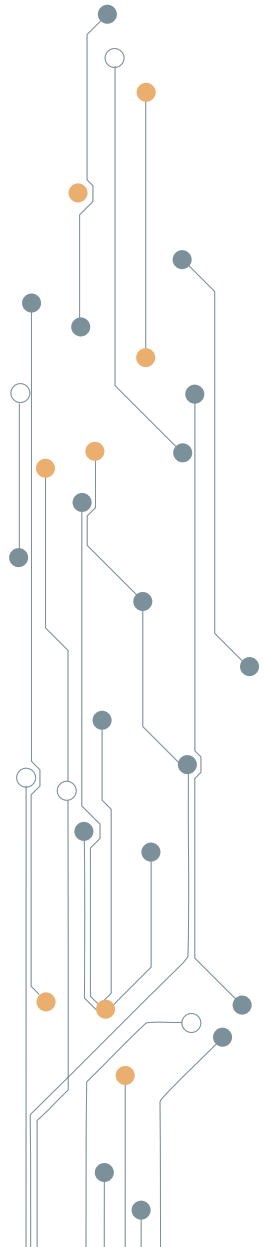
Ataques a redes de datos IPv6

Telefónica EDUCACIÓN DIGITAL

Índice



1. Introducción

Como estudiamos anteriormente IPV6 es un protocolo del nivel 3 de OSI que se desarrolló hace algunos años como alternativa a las problemáticas que están surgiendo en IPv4.

En los contextos de IPv4, un dispositivo se conectaba a una red Ethernet y si quería establecer una comunicación con otra máquina en la red debía saber cómo mínimo la dirección MAC. A continuación, se explican los métodos principales de ataque en IPv6.

No se transmiten físicamente datos entre niveles gemelos. La transferencia se realiza en cada dispositivo, entre capas adyacentes, mediante las interfaces ente capas.

2. Envenenamiento de caché

El primer ataque que vamos a estudiar consiste en un envenenamiento de caché a través de mensajes ICMPv6.
(El protocolo de mensajes de control de internet, o ICMP orientado a IPv6).

Los ataques de envenenamiento de caché tienen el objetivo de hacer pensar a la víctima que la dirección MAC de un dispositivo es una diferente a la que verdaderamente tiene. Man In the Midle, es el ataque más conocido de esta categoría y como ya estudiamos anteriormente, se basaba en la intercepción por parte de un atacante de la comunicaciones de dos dispositivos.

En IPv4, MITM se realizaba a través de mensajes ARP, pero en IPv6 se realizan a través de ICMPv6.

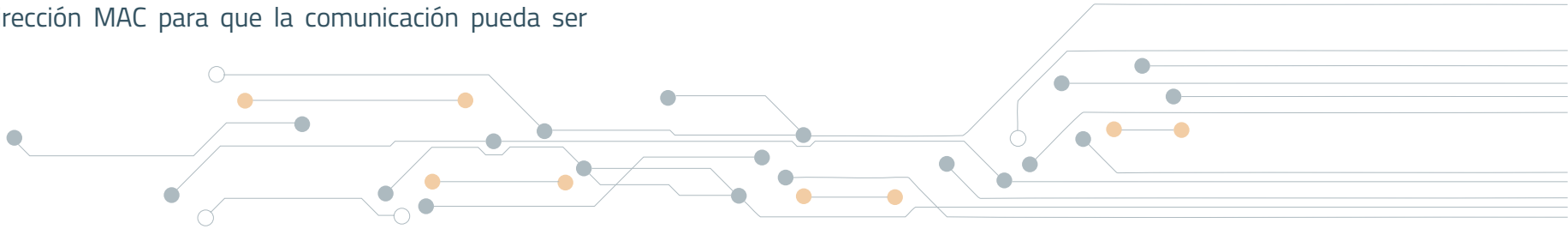
La forma en que se utiliza ICMPV6 para esta función se basa en los mensajes que este protocolo envía preguntando por las direcciones MAC.

De esta forma, cuando un dispositivo A quiere realizar una comunicación con un dispositivo B, A mandará un mensaje de tipo ICMPv6 a una dirección Multicast. El mensaje es denominado “Neighbor Solicitation” y el objetivo es preguntar la MAC de B. Una vez que B ha recibido ese mensaje, responderá con un tipo de mensaje “Neighbor Advertisment” mostrando su dirección MAC para que la comunicación pueda ser viable.

El dispositivo A actualizará su tabla caché, que usará para averiguar las diferentes rutas que necesita seguir para realizar un envío (en este caso con destinatario B).

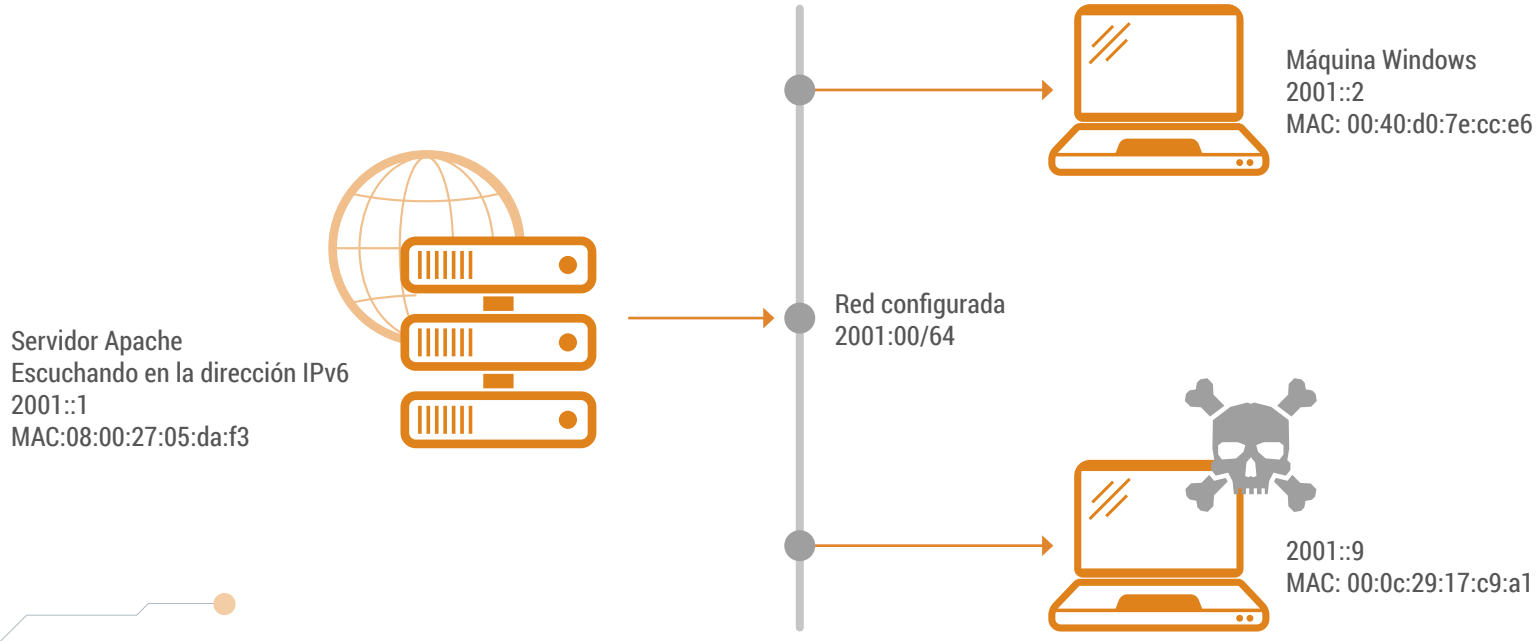
Los ataques Man In the Middle en IPv6 tienen como fundamento el envío periódico de mensajes “Neighbor Advertisment” con datos falsos, previamente modificados por el atacante. Así, el objetivo es actualizar las tablas caché de las víctimas con información maliciosa o manipulada para que las máquinas envíen la información hacia el atacante o la MAC que ha sido introducida en la tabla.

Procedamos a estudiar de forma práctica la explicación anterior.



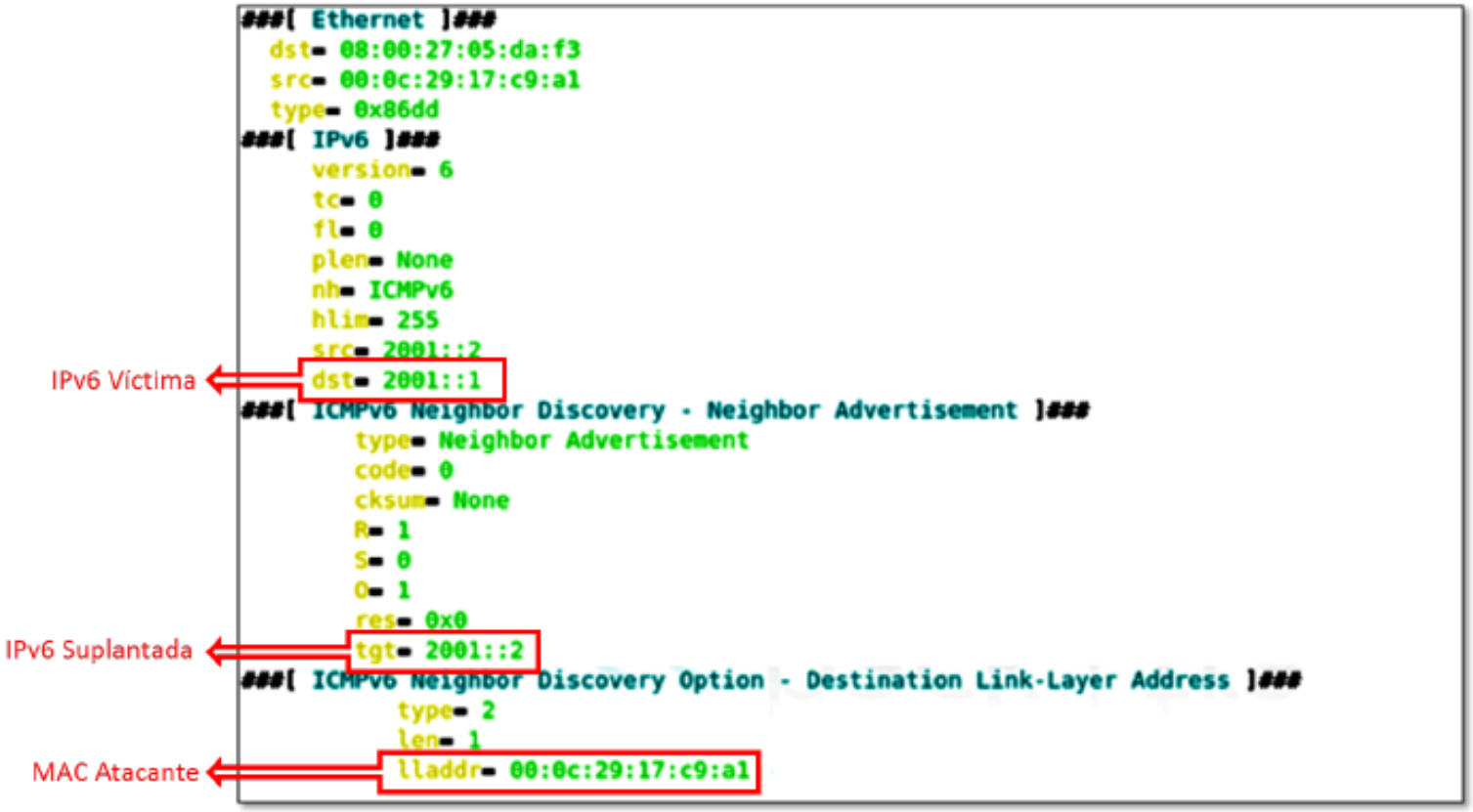
Escenario

Los mensajes que el atacante manda son generados con Scapy, una herramienta de manipulación de paquetes. Aunque hay otras herramientas con las que llevar a cabo este tipo de ataque de forma más sencilla, con Scapy podremos observar más fácilmente los datos de los paquetes.

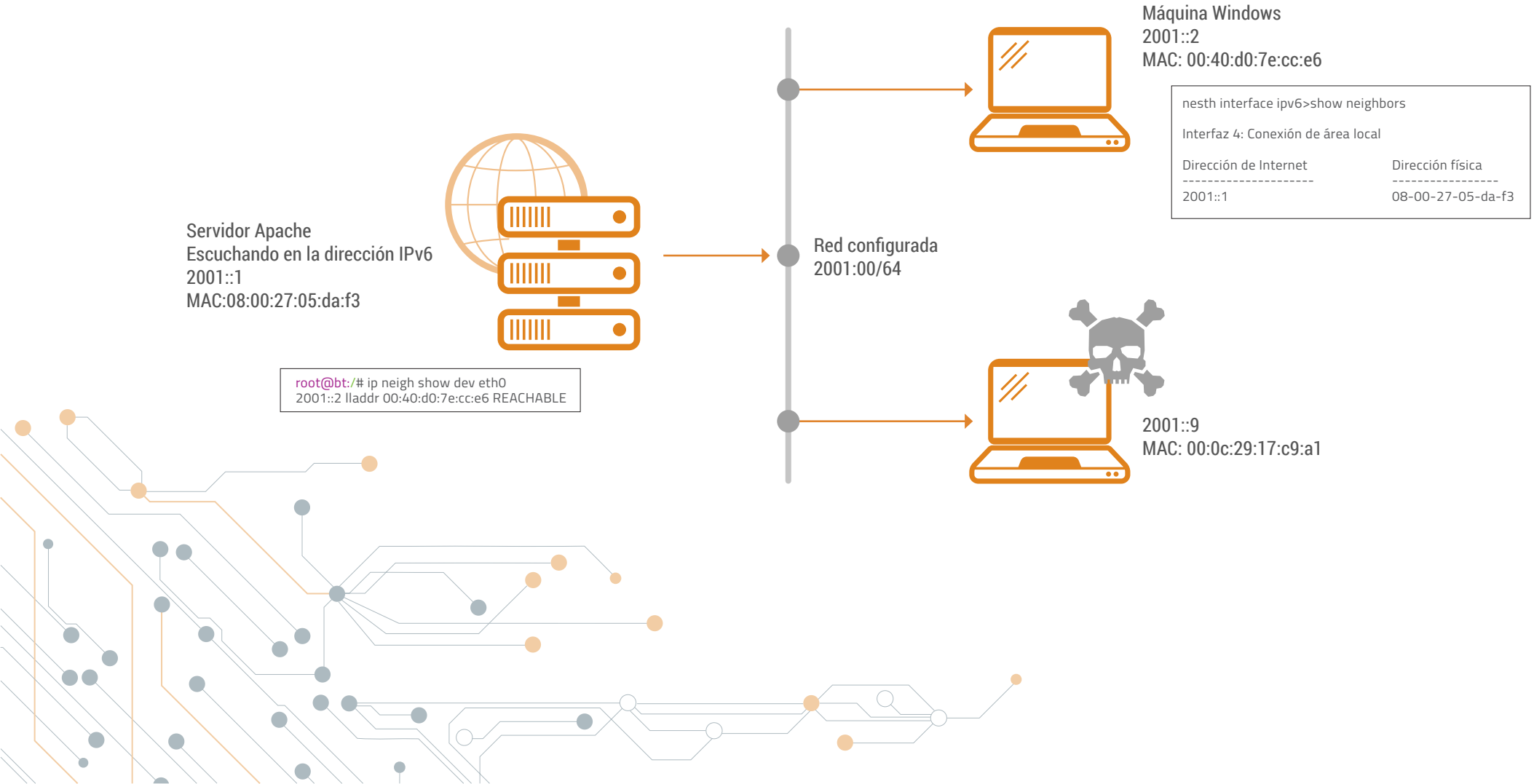


Paquetes enviados hacia la víctima Windows:

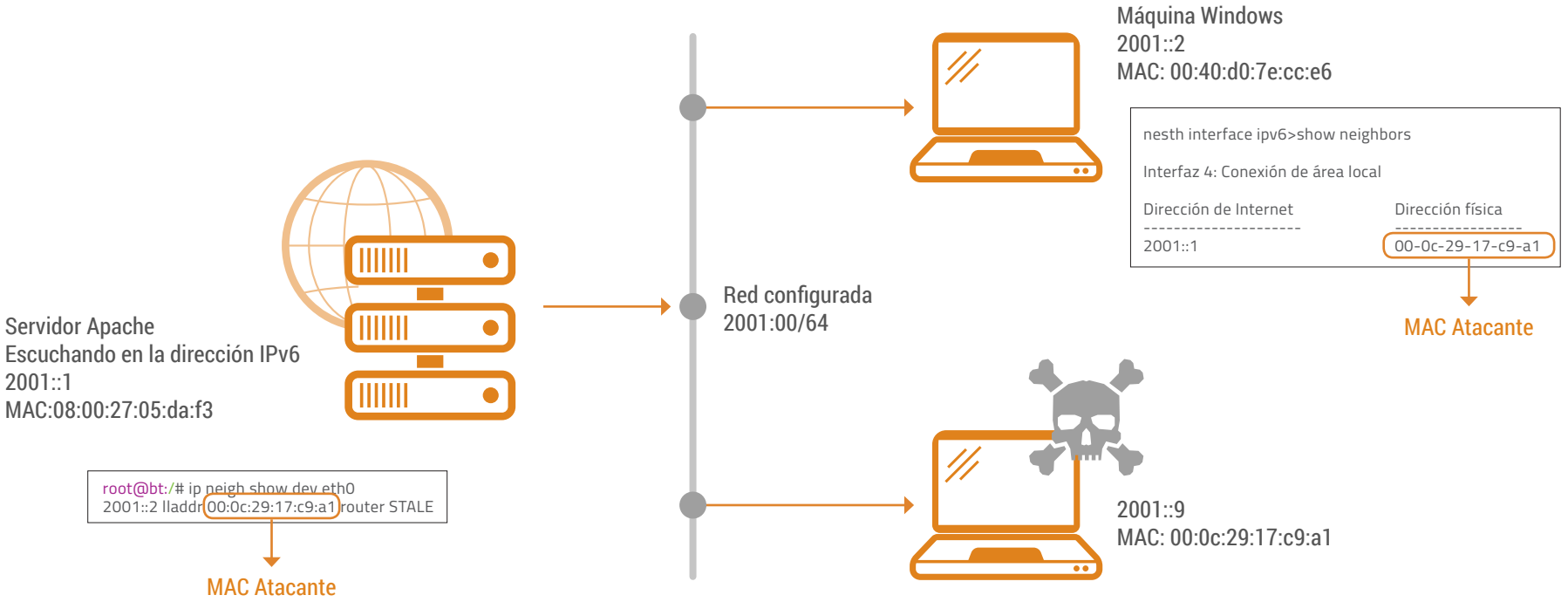
Paquetes enviados hacia el servidor Web:



Cuando el atacante empieza a mandar paquetes en las dos direcciones, las tablas cachés de las máquinas se habrá modificado. Así, el estado en el punto inicial, antes de haber realizado ningún ataque es el siguiente:



Cuando el ataque haya sido realizado las cachés de las máquinas afectadas habrán almacenado la MAC de la máquina del atacante:



Desde ese preciso instante el atacante ya está monitorizando el tráfico entre la víctima y el servidor Web, es decir, puede acceder a él y lo intercepta. Para enviar el tráfico capturado hasta el servidor, es necesario que la máquina del atacante haga forwarding de dichos paquetes, es decir, que los reenvíe hacia el destino final. Esto puede hacerlo modificando el fichero /etc/sysctl.conf y quitando el comentario de la línea:

Net.ipv6.conf.all.fordwarding.
Guardamos el fichero y posteriormente ejecutamos sysctl -p

3. Ataques SLAAC

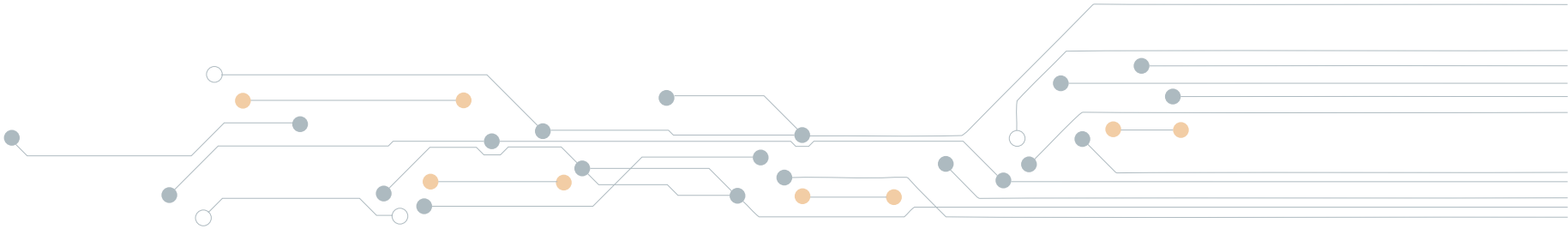
Dentro de las funcionalidades que se aportan en la implementación de IPv6, una de ellas consiste en la posibilidad de realizar una configuración rápida de un adaptador de red donde los parámetros son proporcionados por un router. La capacidad de SLAAC (StateLess Address Auto Configuration) viene definida nuevamente a través de la RFC 4861. Esta permite que en una red enrutada de IPv6, haciendo uso de tramas ICMPv6 se realicen envíos de descubrimiento de enrutador.

A través de la misma y mediante la dirección de vínculo local un cliente podría solicitar y recibir la configuración de la red. Esta operación es diferente de una configuración tipo DHCP puesto que es el router y no el servidor DHCP el que realiza la entrega de la configuración.

Cuando se instala un sistema operativo moderno como Windows 7 o Mac Os X, la implementación predeterminada implica que, tanto IPv4 como IPv6, se encuentren habilitados por defecto y configurados para obtener IP y opciones de red de manera automática.

El ataque de SLAAC consiste en introducir en una red un sistema malicioso que permita proporcionar la información que un equipo puede requerir de SLAAC. Este deber realizar el enrutamiento del tráfico IPv6 hacia Internet para todos los clientes engañados.

De forma predeterminada los sistemas nativos en IPv6 prefieren una comunicación de esta frente a otra en IPv4. Por lo tanto en el caso de una resolución DNS efectiva en IPv6 y una comunicación válida, el tráfico podrá ser enrutado a través del sistema malicioso introducido en la red, en vez del camino legítimo que sería del tipo IPv4.



Puesto que en Internet la comunicación principal se realiza todavía en IPv4 y para que el engaño sea efectivo los clientes tienen que recibir resolución de host en modo IPv6, los sistemas atacantes deben realizar un proceso de conversión IPv4 a IPv6 y viceversa. Esta funcionalidad se consigue a través de NAT-PT.

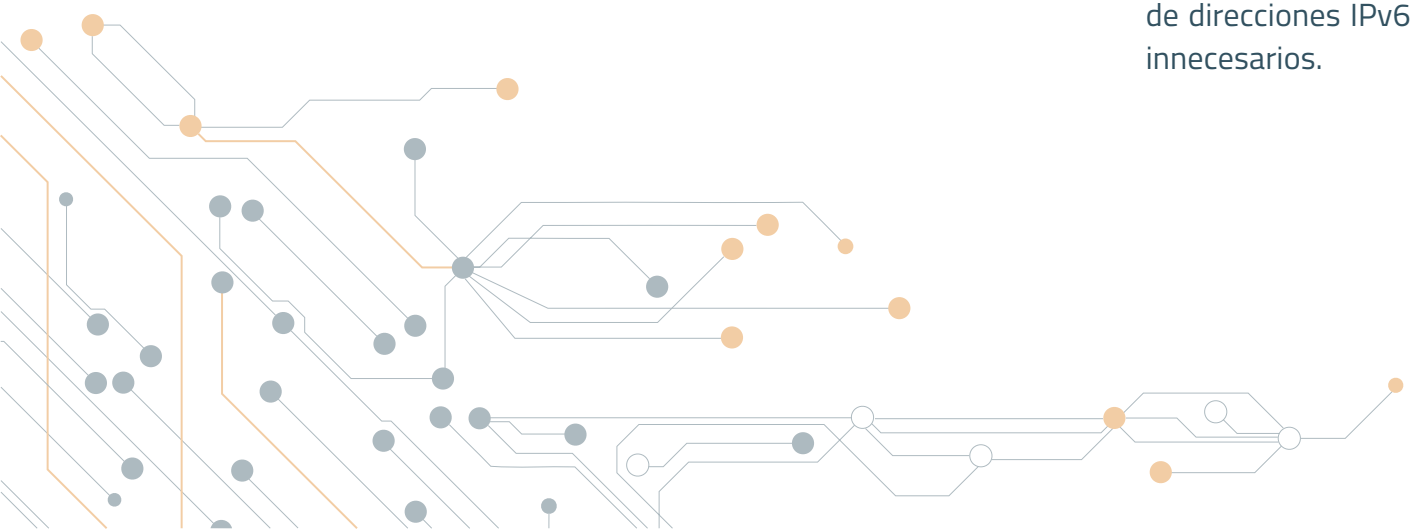
- El cliente realiza a través del sistema router falso una solicitud AAAA de un registro dado.
- El falso router realiza la conversión del registro AAAA en A y la encamina hacia Internet.
- Una vez recibida la solicitud hace la conversión de IPv4 recibida desde un DNS en Internet en una dirección IPv6 que entregará a la víctima.
- La comunicación con esa dirección IPv6 se realizará a través del falso router. En el caso de que no hubiera respuesta o la dirección fuera IPv4 la comunicación se realizaría a través del router legítimo.

Para conseguir el ataque es necesario inicialmente montar un sistema que se encargará de los encaminamientos falsos. Dicho sistema contará con dos adaptadores de red, uno interno con direccionamiento IPv6 y otro IPv4 para la conexión externa hacia Internet.

La funcionalidad de atender las solicitudes y proporcionar los valores de configuración adecuados puede establecerse a través del paquete Radvd.

Una vez que la aplicación ha sido puesta en marcha los clientes que tienen activada la configuración predeterminada de IPv6 recibirán una respuesta a sus peticiones de enrutamientos en IPv6. Para que el ataque sea efectivo será necesario que el router falso pueda realizar la translación de direcciones IPv4 e IPv6. Esto se puede realizar a través de la aplicación naptd existente para distribuciones Linux.

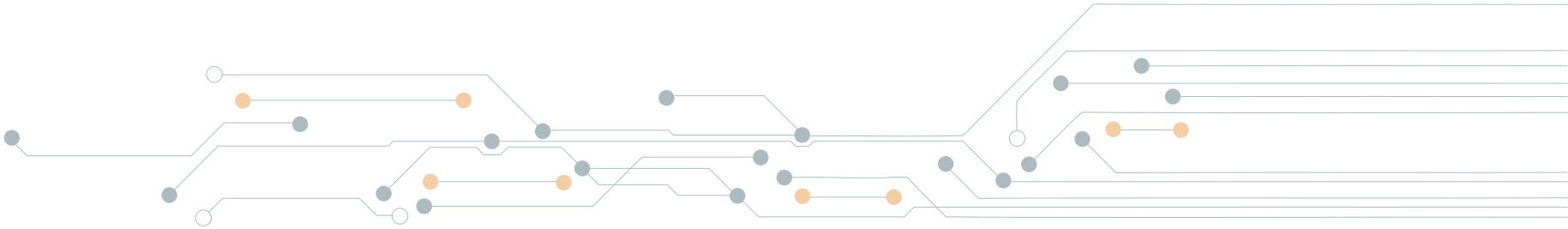
Después de que se haya completado el asistente y lanzada la aplicación habrá que realizar las configuraciones oportunas en las iptables e ip6tables para permitir la translación y enrutamiento de direcciones IPv6 e IPv4, a la vez que se descarten los paquetes innecesarios.



El último paso consistirá en implementar un proxy DNS por ejemplo con totd, para la resolución de los registros solicitados por las víctimas. Ya estará todo dispuesto para que las peticiones pasen a través el atacante. Esto permitirá por lo tanto la reconducción del tráfico de las víctimas produciendo el robo o la modificación del tráfico en tránsito.

Para prevenir el ataque de tipo SLAAC, lo mejor es deshabilitar IPv6 en aquellos adaptadores de red que no vayan a hacer uso del mismo. Esto reduce el vector de ataque teniendo que preocuparse sólo de los ataques de MITM en un escenario de IPv4. Hay que tener en cuenta que aunque en Internet se empiece a funcionar con IPv6, las redes de área local de las organizaciones pueden continuar con la implementación de la versión anterior.

No hay que despreciar ningún adaptador de red, ya que este ataque es también válido para comunicaciones WiFi, lo que hace que pueda ampliarse el alcance de potenciales víctimas.



Telefónica EDUCACIÓN DIGITAL